

#3

11000 U.S. PTO  
09/863583  
05/16/01

**THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re the Application of : Ikuya MORIKAWA, et al.

Filed : Concurrently herewith

For : SYSTEM AND METHOD FOR.....

Serial No. : Concurrently herewith

May 16, 2001

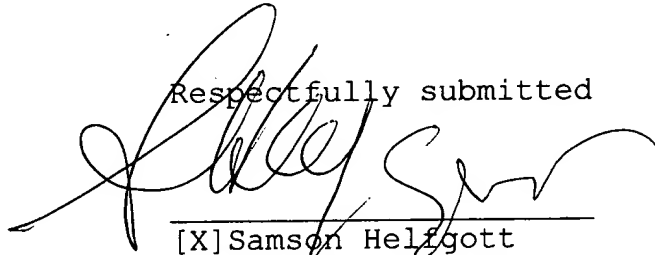
Assistant Commissioner of Patents  
Washington, D.C. 20231

**SUBMISSION OF PRIORITY DOCUMENT**

S I R:

Attached herewith is Japanese Patent Application No.  
2000-145397 of May 17, 2000 whose priority has been claimed in  
the present application.

Respectfully submitted



[X] Samson Helfgott  
Reg. No. 23,072  
[ ] Aaron B. Karas  
Reg. No. 18,923

HELFGOTT & KARAS, P.C.  
60th FLOOR  
EMPIRE STATE BUILDING  
NEW YORK, NY 10118  
DOCKET NO.: FUJA 18.671  
BHU:priority

Filed Via Express Mail  
Rec. No.: EL522402702US  
On: May 16, 2001  
By: Brendy Lynn Belony  
Any fee due as a result of this paper,  
not covered by an enclosed check may be  
charged on Deposit Acct. No. 08-1634.

#3

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

PTO  
09/863583  
U.S. PAT.  
OFFICE  
10/91/50

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日  
Date of Application:

2000年 5月17日

出 願 番 号  
Application Number:

特願2000-145397

出 願 人  
Applicant(s):

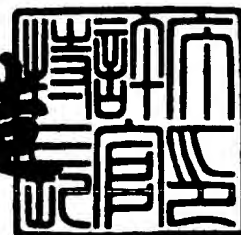
富士通株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年12月15日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 0050917

【提出日】 平成12年 5月17日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G06F 13/00

【発明の名称】 分散グループ管理システムおよび方法

【請求項の数】 5

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 森川 郁也

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 箕浦 真

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 福田 健一

【特許出願人】

    【識別番号】 000005223

    【氏名又は名称】 富士通株式会社

【代理人】

    【識別番号】 100077517

    【弁理士】

    【氏名又は名称】 石田 敬

    【電話番号】 03-5470-1900

【選任した代理人】

    【識別番号】 100092624

【弁理士】

【氏名又は名称】 鶴田 準一

【選任した代理人】

【識別番号】 100100871

【弁理士】

【氏名又は名称】 土屋 繁

【選任した代理人】

【識別番号】 100082898

【弁理士】

【氏名又は名称】 西山 雅也

【選任した代理人】

【識別番号】 100081330

【弁理士】

【氏名又は名称】 樋口 外治

【手数料の表示】

【予納台帳番号】 036135

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9905449

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 分散グループ管理システムおよび方法

【特許請求の範囲】

【請求項 1】 ユーザ側のクライアントと、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバとに対してセキュリティ管理を行うために、ユーザのグループへの所属を間接的に認証する分散グループ管理システムにおいて、

前記リモート処理要求があったとき、当該ユーザが所属するグループ名を含む原グループ情報をもとにグループ証明書をクライアント側で発行するグループ証明書発行装置と、

クライアント側から送信された前記グループ証明書の正当性を前記サーバ内にて検査するグループ証明書検査部と、を備え、

ここに前記グループ証明書発行装置は、該原グループ情報の情報を暗号学的関数により演算した発行側演算値を該原グループ情報に付加して該グループ証明書とし、

前記グループ証明書検査部は、受信した前記グループ証明書に含まれる一部の情報を同一の前記暗号学的関数により演算して検査側演算値を得、前記発行側演算値と前記検査側演算値とが一致することを確認して前記の認証を行うことを特徴とする分散グループ管理システム。

【請求項 2】 前記グループ証明書発行装置は、前記グループに割り当てた秘密情報を前記原グループ情報に含ませて前記暗号学的関数による演算を行い、

前記グループ証明書検査部は、前記グループに割り当てた秘密情報を、受信した前記グループ証明書に含まれる一部の情報に含ませて前記暗号学的関数による演算を行い、

前記グループ証明書発行装置および前記サーバは、同一のグループについて同一の前記秘密情報を相互に共有することを特徴とする請求項 1 に記載の分散グループ管理システム。

【請求項 3】 ユーザ側のクライアントと、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバとに対し

てセキュリティ管理を行うために、ユーザのグループへの所属を間接的に認証する分散グループ管理方法において、

クライアント側で、前記リモート処理要求があったとき、当該ユーザが所属するグループ名を含む原グループ情報の情報を暗号学的関数により演算し、得られた発行側演算値を該原グループ情報に付加したグループ証明書を発行する第1ステップと、

サーバ側で、受信した前記グループ証明書の情報を同一の前記暗号学的関数により演算して検査側演算値を得る第2ステップと、

サーバ側で、前記検査側演算値と受信した前記発行側演算値とを比較し、これらが一致することを確認することにより前記の認証を行い、クライアント側から送信された前記グループ証明書の正当性を前記サーバ内にて検査する第3ステップと、を有することを特徴とする分散グループ管理方法。

【請求項4】 ユーザ側のクライアントと、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバとに対してセキュリティ管理を行うために、ユーザのグループへの所属を間接的に認証する分散グループ管理システムを構成するグループ証明書発行装置であって、

前記リモート処理要求があったとき、当該ユーザが所属するグループ名を含む原グループ情報を発行すると共に、該原グループ情報の情報を暗号学的関数により演算した発行側演算値を該原グループ情報に付加して該グループ証明書とする発行側演算部を備えることを特徴とするグループ証明書発行装置。

【請求項5】 ユーザ側のクライアントと、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバとに対してセキュリティ管理を行うために、ユーザのグループへの所属を間接的に認証する分散グループ管理システムを構成するグループ証明書検査部であって、

前記サーバ側において、クライアント側から受信したグループ証明書に含まれる情報を、暗号学的関数により演算して検査側演算値を生成する検査側演算部を含み、その受信したグループ証明書に含まれる発行側演算値と前記検査側演算値とが一致することを確認して前記の認証を行うことを特徴とするグループ証明書検査部。

## 【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、複数のコンピュータシステム間で分散処理を行う際に、ユーザやユーザの所属するグループに関する情報をセキュリティ管理するための分散グループ管理システムに関する。

近年のコンピュータネットワークの発展により、複数のコンピュータシステム間で分散して情報をやりとりする処理、すなわちリモート処理を行うことが要求されている。このようリモート処理を実行するにあたり、認証の管理およびその認証に基づく権限の管理、すなわちセキュリティ管理は不可欠なものである。

## 【0002】

一方、上記権限についてみると、上記リモート処理を要求するユーザが多数ある場合、それぞれ複数の予め定めたユーザが所属するグループを複数グループ、コンピュータシステム内で設定する、ということが一般に行われている。これが上述したグループであり、これにより多数のユーザの権限、例えばファイルの読出し権限、ファイルの読出し／書込み権限等の権限をきわめて効率良く管理することができる。

## 【0003】

なお上述したグループの概念は、グループ (group) の他に、ロール (role) や特権 (privilege) といった名称でも広く知られているが、本発明においては、これらの名称を代表してグループと称することにする。いずれの名称であっても、一つのグループに複数のユーザが所属できる（場合によっては、一人のユーザが複数のグループに所属できる）といった基本的な性質は同じだからである。

## 【0004】

セキュリティ管理としての現状の認証方式は、(i) パスワードや秘密鍵情報等のような秘密の知識を保持すること、(ii) 例えばICカードのように、物理的な構造を工夫し偽造が困難な物品を所持すること、あるいは(iii) 指紋や網膜パターンのような特定の個人を判別する身体的特徴を利用すること、等を根拠として認証を行うものがほとんどである。

## 【 0 0 0 5 】

ところが、上記の ( i ) ～ ( iii ) に示した認証の根拠をそのまま上記グループの認証に用いようとする、いずれの認証の根拠であっても、上記グループを構成する複数のユーザがそれぞれその認証の根拠を共有することはきわめて困難であり、また、そのグループから脱退するユーザがあるときにそのユーザから、これまで共有していた認証の根拠を剥奪することもきわめて困難である、といった不都合がある。

## 【 0 0 0 6 】

そこでその不都合を解消すべく、まず個人個人のユーザの認証を、上記 ( i ) ～ ( iii ) に示すような認証の根拠に基づいて行った上でさらに、各該ユーザのグループへの所属を別途管理する、という二段階構造のモデルからなるセキュリティ管理手法が採用されている。例えば U N I X のユーザおよびグループを始めとして、多くのコンピュータシステムにおいて、かかるモデルが採用されている。

## 【 0 0 0 7 】

本発明は上記のような、認証に関するセキュリティ管理手法について述べる。

## 【 0 0 0 8 】

## 【従来の技術】

従来の標準的な U N I X は、ユーザおよびグループの概念を有しているが、このグループは、該当するサーバの中にローカルに存在するものである。したがって、このグループが共有する権限を利用することを要求するユーザは、まずユーザ個人としての認証を受けなければならない、という不利がある。

## 【 0 0 0 9 】

一方、上記のユーザおよびグループの概念に関し、N I S ( Network Information Service ) と称される情報共有管理手法が知られている。この手法を用いれば、複数のサーバの各ユーザについて、ユーザ／認証情報テーブルと、ユーザ／グループ対応テーブルと、ユーザ／権限対応テーブルとを、単一の N I S サーバにて一括管理することが可能となる。

## 【 0 0 1 0 】

しかし、その情報共有管理手法を用いても、サーバとNISサーバとの間で緊密な通信が保証されていなければならないことから、セキュリティ管理の主体および組織の枠組みという観点からすると、このNISサーバは、クライアントよりむしろサーバに近い扱いをしなければならない。また、その情報共有管理手法を用いても、上述したユーザ個人としての認証を受けなければならない、という既述の不利が伴うことに変わりはない。

【 0 0 1 1 】

このように、ユーザ個人としての認証を受けなければならない、という上述の不利を解消できる手法の1つとして、間接的に認証を行うという手法が知られている。かかる間接認証手法を主としてUNIXシステムに取り入れたものとして、ケルベロス (Kerberos) と称される分散認証システムが公知文献1において提案されている (公知文献1 : John Kohl and B.Clifford Neuman, The Kerberos Network Authentication Service (Version 5). Internet Request for Comments RFC-1510. September 1993. ) 。

【 0 0 1 2 】

このケルベロス分散認証システムでは、リモート処理を行うサーバではなく、チケットサーバと呼ばれる別のサーバが、各ユーザの直接的な認証を一括して行い、その直接認証を行った上で、本来のサーバの利用を許可するためのチケットを、該チケットサーバより発行する。そして各ユーザは、その発行されたチケットを上記本来のサーバに提示することによって、間接的に認証を受ける仕組みになっている。このような仕組みは、暗号学的手法に基づいて実現されている。

【 0 0 1 3 】

さらに、ケルベロス・バージョン5の拡張フィールドに、グループ所属情報を含める、という提案が公知文献2においてなされている (公知文献2 : B.Clifford Neuman, Proxy-Based Authorization and Accounting for Distributed Systems. In Proceedings of the Thirteenth International Conference on Distributed Computing Systems, pages 283-291, May 1993. ) 。

【 0 0 1 4 】

図48は従来の分散グループ管理システムを表す図 (その1) 、

図 4 9 は同図（その 2）である。

これらの図に示すシステムは、上記公知文献 2 で開示されるケルベロスシステムに、グループへの所属を証明する機能を付加したシステム構成を表す。ただし、後述する本発明のシステム構成と対比しやすいような構成にして表している。

【0015】

上記公知文献 2 を参照すると、チケットは前述のグループ所属情報とは別に、ユーザ（U）個人のユーザ名の情報も含むが、サーバ 1 側では必ずしもこのユーザ名を使わなくとも、該グループ所属情報だけで、認証と権限の適用とが行えるので、図 4 8 および 4 9 では、サーバ 1 が保持しうるユーザ U に関する情報を省略している。

【0016】

このように、前述した間接認証の仕組みに、グループ所属情報を取り入れることによって、ユーザーグループの管理をサーバ 1 から切り離して一括して行い、これにより、ユーザ（U）個人としてはサーバ 1 にこれを登録することを不要とした分散グループ管理システムが実現される。

図 4 8 および 4 9 に示すシステムをより一層詳しく説明すると次のとおりである。

【0017】

本図において参照番号 1 0 は分散グループ管理システムを表し、サーバ 1 と、クライアント 2 と、チケットサーバ 3' とにより構成され、これらの構成要素 1, 2 および 3' は、ネットワーク 4 を介して相互に通信可能である。

通常クライアント 2 は複数存在し（図では簡単のために 1 つのみ示す、以下同様）、しかも多数のユーザ U がこれらのクライアント 2 およびネットワーク 4 を介して、サーバ 1 に対しリモート処理を要求する。

【0018】

各ユーザがどのグループに所属するかというグループメンバーシップを表すテーブルは、全ユーザに対し一括してチケットサーバ 3' が保持する。図では、ユーザーグループマッピング格納手段 3 2 がそのテーブルの機能を果たす。

ユーザ U がクライアント 2 を介してサーバ 1 に対しリモート処理を要求するに

際し、ユーザUはまずチケットサーバ3' に対しチケットTCの発行を要求する。ただし、この要求のための経路は図示を省略している（以下の各図において同じ）。チケットサーバ3' はその要求を受けて、そのユーザが例えば「グループ1～グループ4」のうち、例えば「グループ2」に所属していること（予め手段32に登録している）を、該ユーザーグループマッピング格納手段32より知ると、この「グループ2」を含むチケットTCをチケット発行部31' より発行し、クライアント2に返す。ユーザはこのチケットTCを持ってサーバ1に対しアクセスし、リモート処理を要求する。

【0019】

これを受けてサーバ1は、認証機能部11にて当該アクセスに対する認証を行い正当なアクセスか否か判断する。この判断に際し、チケット検査部12' は受信したチケットTCの検査を行う。

このチケットTCの検査にて、当該アクセスが「グループ2」についてのリモート処理要求であることを知ると、サーバ1は、グループ権限マッピング格納手段15を参照して、「グループ2」に許可された権限が例えば“ファイルからの読出しのみ”であるとする（予め登録してある）、その権限内での当該リモート処理を実行する。

【0020】

なお、チケットサーバ3' 内のグループ秘密情報格納手段33は、サーバ11内のグループ秘密情報格納手段13と協働して一層セキュリティを高めるべく、各グループ毎に予め付与された秘密情報（秘密コード）をお互いに持ち合う。また、チケット蓄積部14' は、受信したチケットTCを一時的に蓄積して保持し、悪意の第三者によりなされたりリモート処理要求か否かを判断するのに用いられる。

【0021】

このような悪意の第三者が、ユーザからのチケットTCを、例えばネットワーク4上にて盗み見し、「グループ2」から「グループ3」（「グループ3」に与えられた権限は、例えば“ファイルからの読出しおよびファイルへの書込みの双方”であるものとする）への改ざんを試みたとなると、その悪意の第三者によっ

て、そのファイルの中身が書き換えられてしまう、という事態が発生してしまう。

#### 【0022】

セキュリティ管理上かかる事態の発生は可能な限り抑止しなければならない。そのために設けられたのが、チケット発行部31'内の暗号化機能部34'であり、チケットTCを上記秘密コードを秘密鍵として用いて暗号化した上でクライアント2に返す。

暗号化されたチケットTCはネットワーク4に送出され、これを受信したサーバ1は、復号化機能部16'にて上記秘密コードを秘密鍵として用いて復号し元のチケットTCに戻す。このような暗号化処理によりセキュリティは大幅に向上される。

#### 【0023】

##### 【発明が解決しようとする課題】

上記暗号化機能部34'による暗号化処理は、原チケットTCに対し秘密鍵をもって暗号化することにより行われる。したがって、秘密鍵が悪意の第三者に知られない限り、原チケットTCを盗み見することはきわめて困難であり、セキュリティは確保される。

#### 【0024】

しかしながら、一般に、上記暗号化処理のための処理速度は遅く、かなりの処理時間を要してしまう。このため、グループの間接認証を高速に行うことができない、という問題がある。

したがって本発明は、上記問題点に鑑み、グループの間接認証を高速化できる分散グループ管理システムを提供することを目的とするものである。

#### 【0025】

##### 【課題を解決するための手段】

図1は本発明に基づく分散グループ管理システムの基本構成を示す図である。なお全図を通して同様の構成要素には、同一の参照番号または記号を付して示す。

本図において、参照番号10は分散グループ管理システムを表す。このシステ

ム 1 0 は、ユーザ (U) 側のクライアント 2 と、各グループ毎に割り当てられた所定の権限 (authorization) のもとにユーザ側からのリモート処理要求を実行するサーバ 1 とに対してセキュリティ管理を行うために、ユーザ U のグループへの所属を間接的に認証 (authentication) するものである。

#### 【 0 0 2 6 】

このシステム 1 0 は、サーバ 1 と、クライアント 2 と、グループ証明書発行装置 3 と、これらの間の相互通信に供するネットワーク 4 とからなる。さらにサーバ 1 側には、グループ証明書検査部 1 2 が設けられる。

グループ証明書発行装置 3 は、リモート処理要求があったとき、当該ユーザが所属するグループ名を含む原グループ情報 G R をもとにグループ証明書 G C (Group Certificate) をクライアント 2 側で発行し、

グループ証明書検査部 1 2 は、クライアント 2 側から送信されたグループ証明書 G C の正当性をサーバ 1 内にて検査する。

#### 【 0 0 2 7 】

ここにグループ証明書発行装置 3 は、原グループ情報 G R の情報を暗号的関数 (cryptographic function) により演算した発行側演算値をこの原グループ情報 G R に付加し、グループ証明書 G C とする。またグループ証明書検査部 1 2 は、受信したグループ証明書 G C に含まれる一部の情報を同一の上記暗号的関数により演算して検査側演算値を得、これら発行側演算値と検査側演算値とが一致することを確認して、前述の認証を行う。

#### 【 0 0 2 8 】

上記本発明の分散グループ管理システム 1 0 は、次に述べる分散グループ管理方法としても捉えることができる。

図 2 は本発明に基づく分散グループ管理方法の基本ステップを示す図である。

本図に示すとおり、その方法は第 1 ステップ S 1 と、第 2 ステップ S 2 と、第 3 ステップ S 3 とを有する。この方法は、ユーザ (U) 側のクライアント 2 と、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバ 1 とに対してセキュリティ管理を行うために、ユーザ U のグループへの所属を間接的に認証する分散グループ管理方法であって、

(i) 第1ステップS1では、クライアント2側で、リモート処理要求があったとき、当該ユーザUが所属するグループ名を含む原グループ情報GRを暗号学的関数により演算し、得られた発行側演算値を原グループ情報に付加したグループ証明書GCを発行する。

【0029】

(ii) 第2ステップS2では、サーバ1側で、受信したグループ証明書GCの情報を同一の暗号学的関数により演算して検査側演算値を得る。

(iii) ステップS3では、サーバ1側で、検査側演算値と受信した発行側演算値とを比較し、これらが一致することを確認することにより上述の認証を行い、クライアント2側から送信されたグループ証明書GCの正当性をサーバ1内にて検査する。

【0030】

従来は、既に述べたとおり、グループ名等の情報を含むメッセージデータ（チケットTCに相当）を、秘密鍵により暗号化して暗号文を得る。そしてクライアント側から送信されたその暗号文を、サーバ側にてその秘密鍵により復号して元のメッセージデータを再生している。すなわち、元のメッセージデータを全く別の暗号文に変換して送信し、受信したその暗号文を元のメッセージデータに変換し直すという大規模な処理を行っている。このために、チケットTCの生成にかなりの時間を要した。

【0031】

ところが本発明ではグループ名等を含むメッセージデータを全く別のデータに変換するということはせず、したがって、元のメッセージデータにまた戻すということもしない。このため伝送されるメッセージデータは実質的に生データのままである。単に送信するメッセージデータに暗号学的関数の演算を施して得た発行側演算値をこのメッセージデータに付加し、受信側でもそのメッセージデータに同一の暗号学的関数の演算を施して個別に検査側演算値を生成して、これら演算値が一致するか否かを検査するのみである。もし一致していなければ、メッセージデータをクライアント側から送信してからサーバ側で受信するまでの間に、悪意の第三者により、そのメッセージデータが一部改ざんされたものと推測する

ことができる。したがって、サーバ 1 は当該リモート処理要求を受け付けない。

【0032】

上記のような暗号学的関数としての好適例の 1 つとしては、暗号学的ハッシュ関数 (hash function) を挙げることができ、この関数はシンプルなアルゴリズムで実現される。以下の説明では、この暗号学的ハッシュ関数 (以下、単にハッシュ関数とも称す) を例にとり行う。この場合、このハッシュ関数それ自体は既知であるため、上記の発行側演算値が悪意に再生される可能性は否定できない。このような恐れに確実に対処するための一例として、秘密情報を利用することができる。この秘密情報を利用した場合の本発明の分散グループ管理システムは、次のように構成することができる。再び図 1 を参照すると、

グループ証明書発行装置 3 は、グループに割り当てた上記の秘密情報を原グループ情報 GR に含ませて暗号学的関数 (ハッシュ関数) による演算を行う。また、グループ証明書検査部 12 は、グループに割り当てた秘密情報を、受信したグループ証明書に含まれる一部の情報に含ませて暗号学的関数 (ハッシュ関数) による演算を行う。ここに、グループ証明書発行装置 3 およびサーバ 1 は、同一のグループについて同一の秘密情報を相互に共有するようにする。

【0033】

このようにすると、上記秘密情報は上記装置 3 と検査部 12 のみが保有するものであるから、この秘密情報を知らない第三者は同一の発行側演算値 (ハッシュ値) を得ることはできない。この場合、盗み見たハッシュ値から元のグループ証明書の内容を再現することは不可能であり、これがハッシュ値を採用する利点でもある。なお、以下の説明では、上記の秘密情報を用いた場合を例にとり行う。

【0034】

【発明の実施の形態】

〔第 1 実施例〕

図 3 は本発明に基づく第 1 実施例を示す図 (その 1)、

図 4 は同図 (その 2) である。

なお、この第 1 実施例に続いて後に、第 2 実施例から第 7 実施例まで説明する

が、いずれの実施例においても、グループ証明書発行装置 3、およびサーバ 1 内のグループ証明書検査部 1 2 は基本的に次のような構成からなる。

【 0 0 3 5 】

前者 ( 3 ) は、ユーザ側のクライアント 2 と、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバ 1 とに対してセキュリティ管理を行うために、ユーザ U のグループへの所属を間接的に認証する分散グループ管理システムを構成するグループ証明書発行装置であって、その特徴とするところは、上記のリモート処理要求があったとき、当該ユーザが所属するグループ名を含む原グループ情報 G R を発行すると共に、この原グループ情報 G R の情報を暗号学的関数 ( ハッシュ関数 ) により演算した発行側演算値を、この原グループ情報 G R に付加してグループ証明書 G C とする発行側演算部 ( 3 4 ) を備える点にある。

【 0 0 3 6 】

一方後者 ( 1 2 ) は、同様に、ユーザ側のクライアント 2 と、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバ 1 とに対してセキュリティ管理を行うために、ユーザ U のグループへの所属を間接的に認証する分散グループ管理システムを構成するグループ証明書検査部であって、その特徴とするところは、サーバ 1 側において、クライアント 2 側から受信したグループ証明書 G C に含まれる情報を、暗号学的関数 ( ハッシュ関数 ) により演算して検査側演算値を生成する検査側演算部 ( 1 6 ) を含み、その受信したグループ証明書 G C に含まれる発行側演算値と前述の検査側演算値とが一致することを確認して上記の認証を行う点にある。

【 0 0 3 7 】

図 3 および図 4 を参照すると、

サーバ 1 と複数のクライアント 2 ( 簡単のため、1 つのみ示す ) が、ネットワーク 4 によって接続されている。サーバ 1 は認証機能部 1 1、グループ証明書検査部 1 2、グループ秘密情報格納手段 1 3、グループ証明書蓄積部 1 4 およびグループ権限マッピング格納手段 1 5 を有する。

【 0 0 3 8 】

グループ証明書発行装置 3 はネットワーク 4 に接続されていて、グループ証明書発行部 3 1、ユーザーグループマッピング格納手段 3 2 およびグループ秘密情報格納手段 3 3 を有する。

グループ証明書発行装置 3 とサーバ 1 は、グループ名の名前空間の一部を共有しており、そのように共有されているグループ名に割り当てられているグループの前述した秘密情報として相互に対応した値を、グループ証明書発行装置 3 のグループ秘密情報格納手段 3 3 およびサーバ 1 のグループ秘密情報格納手段 1 3 内にそれぞれ保持している。またグループ証明書発行装置 3 とサーバ 1 はそれぞれ図示されていない時計機能を持っており、両者は完全にあるいはある小さな誤差の範囲で同期しているものとする。

#### 【 0 0 3 9 】

クライアント 2 のユーザ U がサーバ 1 へリモート処理を要求する際には、まず接続したいサーバ 1 の名前（サーバ名）と、グループ証明書発行装置 3 へ登録されている自らのユーザ名とを、グループ証明書発行装置 3 へ送信することで、グループ証明書 G C の発行を要求する（ただしこのプロセスは図 3 内で矢印として図示されていない）。グループ証明書発行装置 3 内のグループ証明書発行部 3 1 はこれを受け取り、ユーザーグループマッピング格納手段 3 2 より得られるユーザに割り当てられたグループ名、グループ秘密情報格納手段 3 3 より得られるそのグループに割り当てられた秘密情報、および現在の時刻から算出される有効期限情報（有効期限は、割り当てられたグループの権限を使用する期間）を原グループ情報 G R とし、これらの値を、前述した発行側演算部をなすハッシュ機能部 3 4 により処理（ハッシュ関数の演算等）してグループ証明書 G C を作成する。そしてこれをクライアント 2 へ返送する。

#### 【 0 0 4 0 】

そのグループ証明書 G C を得たクライアント 2 は、これを、ネットワーク 4 を介し、サーバ 1 へ送信する。サーバ 1 では、グループ証明書検査部 1 2 においてグループ秘密情報格納手段 1 3 とグループ証明書蓄積部 1 4 を用いて、受け取ったグループ証明書 G C の正当性を検査し、正当であればグループ証明書蓄積部 1 4 へそのグループ証明書 G C を格納する。この検査は、前述した検査側演算部を

なすハッシュ機能部 1 6 が、ハッシュ関数演算の演算結果をもとに行う。

【 0 0 4 1 】

上記の検査の成功をもって認証機能部 1 1 は認証の完了と見なし、グループ証明書 G C 内に示されたグループを、グループ権限マッピング格納手段 1 5 において照合し、このグループに与えられた権限を認識する。この権限の範囲内でクライアント 2 のユーザ U から要求されたりリモート処理を実施する。

図 5 は本発明に基づく第 1 実施例を適用した全体構成例を示す図（その 1）、

図 6 は同図（その 2）である。

【 0 0 4 2 】

なお、後述する第 1 実施例～第 7 実施例を適用した全体構成例も、図 5 および図 6 に示したのと同様になる。

図 5 および図 6 において、組織 A と組織 B の各計算機システムが、ネットワーク 4 で接続されており、グループ証明書発行装置 3 は組織 A が、サーバ（サーバ名を s e r v e r X とする）1 は組織 B が管理している。

【 0 0 4 3 】

サーバ 1 は自組織 B 内のユーザ向けに、ユーザパスワード格納手段 1 7、ユーザ権限マッピング格納手段 1 8 およびユーザグループマッピング格納手段 1 9 を備えており、これらには組織 B のユーザが登録されている。組織 B のユーザは自組織 B 内のクライアント 2, 5 から、サーバ 1 におけるユーザ名と認証情報をライン L 3 を介し送信し、認証を受けてからリモート処理を要求する。

【 0 0 4 4 】

これに対し組織 A のユーザは、サーバ 1 内の上記各格納手段 1 7, 1 8 および 1 9 には登録されていないので、自組織 A 内のグループ証明書発行装置 3 に、ライン L 1 を介して、グループ証明書 G C を発行してもらい、これをサーバ 1 に、ライン L 2 を介して、送信することにより、リモート処理を要求することができる。

【 0 0 4 5 】

すなわち、組織 B のユーザは、従来の方法でリモート処理を依頼する一方、組織 A のユーザは、組織 B のサーバ 1 に各々のユーザ情報（ユーザ名、パスワード

、権限等）が登録されていなくても、グループ証明書GCによって、リモート処理を依頼することができる。

図7はパスワード格納手段21内のデータ構成例を示す図である。

#### 【0046】

この格納手段21は、図5に示すグループ証明書発行装置3内に設けられている。その格納データは、自組織A内におけるユーザ名例えばuser A, user B, …と各ユーザ毎に対応するパスワード例えばpassword A, password B, …の組からなる。パスワードは、各ユーザと装置3との間で秘密裏に共有されているものとする。

#### 【0047】

図8はユーザーグループマッピング格納手段32内のデータ構成例を示す図である。

この格納手段32は、図3および図5に示すグループ証明書発行装置3内に設けられている。その格納データは、ユーザ名例えばuser A, user B, …と、そのユーザ毎に割り当てられたグループ名例えばgroup 3, group 1, …の組からなる。

#### 【0048】

グループ証明書発行装置3は、server X1つだけでなく、図示されないserver X以外のサーバとの間でも分散グループ管理を一括して行えるため、この例ではユーザ名の項目を、サーバ名と自組織Aでのユーザ名の組としてある。またグループ名についても、どのサーバにおけるグループ名かを明らかにするために、サーバ名が付与してある。

#### 【0049】

図9はグループ秘密情報格納手段33内のデータ構成例を示す図である。

この格納手段33は、図5に示すグループ証明書発行装置3内に設けられている。その格納データは、サーバにおけるグループ名と、そのグループ毎に割り当てられた既述の秘密情報例えばsecret 1, secret 2, …との組からなる。各組は、対応するサーバ1のグループ秘密情報格納手段13（図6）内の各組と共有されていなければならない、そのようにして共有されているグループの

秘密情報は、グループ証明書発行装置 3 とサーバ 1 との間で、秘密裏に共有されていなければならない。ネットワーク 4 上には秘密情報を流さないようにするためである。

#### 【0050】

図 10 はグループ秘密情報格納手段 13 内のデータ構成例を示す図である。

この格納手段 13 は、図 4 および図 6 に示すサーバ (server X) 内に設けられている。その格納データは、サーバ (server X) 自らが取り扱うグループ名と、そのグループ毎に割り当てられた秘密情報との組からなる。各組は、前述のとおり、グループ証明書発行装置 3 内のグループ秘密情報格納手段 33 との間で共有されている。

#### 【0051】

なお、図 10 のテーブルの左項のグループ名は、グループ証明書発行装置 3 ではサーバ名が付与されたものであったが、サーバ 1 では、付与されるべきサーバ名は自身の名前（ここでは server X）であるのは自明であるので、省略されている。

図 11 はグループ権限マッピング格納手段 15 内のデータ構成例を示す図である。

#### 【0052】

この格納手段 15 は、図 4 および図 6 に示すサーバ (server X) 1 内に設けられている。その格納データは、グループ名と、そのグループ毎に割り当てられた権限との組からなる。本図の例では、権限は、リモート処理対象の名前と、その処理対象の各々に対して許可される処理内容の種類との組からなる。この例では、処理対象はファイル名であって、処理内容は読出しを表す「r」および書込みを表す「w」としている。すなわち「r」は読出し許可を表し、「w」は書込み許可を表し、「-」はそれぞれの不許可を表す。

#### 【0053】

なおリモート処理権限としての、ファイルの読出しや書込みの許可／不許可は一例であってこれに限るものではない。他の例としては、プリンタ使用の許可／不許可等もある。また、許可／不許可に限らず、リモート処理時の動作の様式を

ユーザやグループごとに指定した設定の類も、このリモート処理権限に含まれる。

#### 【0054】

次に、本発明において注目すべき特徴の1つであるグループ証明書GC（図1、図3および4、図5および6等）について詳しく説明する。

図12は第1実施例でのグループ証明書GCの具体的生成方法を示す図である。以下の説明では、ユーザU（user B）が、サーバ1（server X）におけるリモート処理のために、グループ証明書GCの発行を求めた場合を仮定する。そしてuser Bにはgroup 1が割り当てられているものとする。

#### 【0055】

まず、グループ名group 1、有効期限情報timestamp、グループの秘密情報secret 1の3つからなる原グループ情報GRを、何らかの可逆な方法（受け取り側で再現可能な方法）で結合する。この結合を、ここでは「|」という記号で表す。

次に、上記のGRに暗号的ハッシュ関数Hを適用して、テンポラリパスワードtempを生成する。本図の例では、それぞれの値は文字列で表現されるものとし、グループ名にはサーバ名が付与され、有効期限情報は年月日および時刻の“時と分”の情報をそれぞれ2桁ずつで並べたものとしているが、この限りでない。また上記秘密情報は、グループ証明書発行装置3のグループ秘密情報格納手段33から得られる。

#### 【0056】

かくして得られたGRにハッシュ関数Hを適用し、その結果（ハッシュ値）をテンポラリパスワードtempと呼ぶこととする。すなわち、

$$temp = H(group\ 1 | timestamp | secret\ 1)$$

である。

ハッシュ関数Hは暗号的ハッシュ関数と呼ばれるものであり、暗号的・計算量的な一方向性（すなわちxから $y = H(x)$ を求めるのは容易だが、 $y = H(x)$ からxを求めるのは非常に困難なこと）と、コリジョンフリー性（すなわち $H(x) = H(z)$ となるようなxと異なるzの値が存在しないか、あるいは

発見が非常に困難なこと)といった性質を持つ。このようなハッシュ関数としては、MD5やSHA1などが挙げられる。

#### 【0057】

グループ証明書GCは、GRと同じグループ名group1および有効期限情報timestampに対し、上記ハッシュ値であるテンポラリパスワードtempを結合したものである。図3および図5に示すグループ証明書発行装置3は、そのGCをユーザ(userB)Uへ返送する。

上述のとおり、第1実施例のもとでのグループ証明書発行装置3において発行側演算部(ハッシュ機能部34)は、少なくともグループ名およびそのグループに固有の秘密情報に対し一括してハッシュ関数Hの演算を適用し、得られた発行側演算値(ハッシュ値)をテンポラリパスワードtempとなし、少なくともグループ名およびテンポラリパスワードからグループ証明書GCを生成する。

#### 【0058】

図13は第1実施例でのグループ証明書GCの具体的検査方法を示す図である。

サーバ1側でのグループ証明書GCの検査は、与えられた情報から同じようにグループ証明書GCを生成してみて、同じ結果になるかどうかを確認することで実現する。すなわち、受け取ったグループ証明書GCからグループ名と有効期限情報とを取り出し、これらの情報に、サーバ1内のグループ秘密情報格納手段13から取得した当該グループ(group1)の秘密情報を結合し、クライアント側と同様に、全体にハッシュ関数Hを適用する。そして、その結果の再現されたテンポラリパスワードtemp'を、上述の受け取ったグループ証明書GCに含まれているテンポラリパスワードtempと比較手段20(例えば図4の検査部12に形成される)において比較し、両者が等しければグループ証明書GCは、例えばネットワーク4上で偽造や改ざん等を施されていない正当なものだと分かる。なぜなら、もしグループ証明書内の情報の一部でも変更されていれば、前述したハッシュ関数Hの性質により、両者は等しくなり得ないからであり、かつ、そのハッシュ関数Hの性質により、テンポラリパスワードが等しくなるような改ざんは不可能か非常に困難であるからである。

【0059】

上述のとおり、第1実施例のもとでのグループ証明書検査部12において検査側演算部（ハッシュ機能部16）は、クライアント側から受信したグループ証明書GCに少なくとも含まれるグループ名およびそのグループに固有の秘密情報に対し一括してハッシュ関数Hの演算を適用することにより検査側演算値（ハッシュ値）を、再現されたテンポラリパスワードtemp'として再生する。

【0060】

結局、上記第1実施例の分散グループ管理システム10においては、以下の図14～図16に図示するような処理が行われることになる。

図14は第1実施例のもとでの全体の処理の流れを表す図（その1）、

図15は同図（その2）である。

これらの図の処理の流れを、図5および図6を参照しながら説明する。

【0061】

まずクライアント2はユーザ名userBと、リモート処理を要求したいサーバ名serverXと、パスワードpasswordBの3つを、グループ証明書発行装置3へ送信する。

グループ証明書発行装置3は、まず認証機能部22によりパスワードを照合してユーザ1を認証してから、受け取ったサーバ名serverXと、ユーザ名userBとを、ユーザーグループマッピング格納手段32にて照合し、このuserBに割り当てられているグループ名group1を取得する。

【0062】

次にグループ証明書GCを、グループ名groupBと、有効期限情報timestampと、秘密情報とから、前述の方法で生成する。なお有効期限の決定方法は本発明では特に定めないが、期間が長くても短くてもそれぞれ欠点があるので、適切に決定する。こうして生成されたグループ証明書をユーザへ返送する。以上の処理を、“グループ証明書獲得フェーズ”と称することにする。

【0063】

クライアント2がサーバ1へリモート処理を要求するには、このグループ証明書GCをサーバ1へ送信すればよい。このグループ証明書GCを受け取ったサー

バ 1 では、まずグループ証明書検査部 1 2 がその受け取ったグループ証明書を検査する。検査の詳しい方法は図 1 6 で述べるが、その検査の結果、正しいものであると判断されると、グループ証明書 G C に含まれるグループ名は正しいものと見なされ、そのグループ名を用いてグループ権限マッピング格納手段 1 5 から、対応する権限を得るのに用いられる。以上の処理を、“ログインフェーズ”と称することになると、これ以後に目的とするリモート処理が実行される。

#### 【 0 0 6 4 】

図 1 6 は第 1 実施例のもとでのグループ証明書検査部 1 2 の動作の流れを示す図である。まず、受け取ったグループ証明書 G C を逐次蓄積するグループ証明書蓄積部 1 4 を検索し、有効期限の切れていないグループ証明書 G C のうちで、今回受け取ったグループ証明書 G C と同じテンポラリパスワード t e m p を有するものがないか調べる（ステップ S 1 1）。

#### 【 0 0 6 5 】

もしあれば、受け取ったグループ証明書 G C は不正に二重使用されたものであるから、当該リモート処理要求を拒否する（ステップ S 1 2 および S 1 7）。もしなければ、受け取ったグループ証明書 G C をグループ証明書蓄積部 1 4 に追加する（ステップ S 1 2 および S 1 3）。

次に上述の受け取ったグループ証明書 G C を検査し、もし正しいものであれば（ステップ S 1 4 および S 1 5）、認証機能部 1 1 に検査に合格したことを通知する（ステップ S 1 6）。

#### 【 0 0 6 6 】

なお、この第 1 実施例ではグループ証明書発行装置 3 とユーザとの間の認証はパスワードにより行っているが、認証方法はこの限りでない。もしグループ証明書発行装置 3 とユーザとの間での不正はあり得ないと仮定できる場合には、認証をしなくても構わないし、パスワード以外の他の信頼できる方法、たとえば身体的特徴を利用したり、あるいはクライアントのホストアドレスを利用することでも構わない。一方、グループ証明書発行装置 3 とユーザとの間の途中経路（ライン L 1）が安全でなく、そこでの盗み見や改ざんがあり得るのであれば、ケルベロスにおいて行われているのと同様に両者間で暗号鍵を共有して暗号通信により

認証と盗み見や改ざんに対する防御を兼ねても構わない。

【0067】

以上述べたとおり、第1実施例では、ハッシュ関数Hを適用することでグループ証明書GCを生成および検査するものであり、ハッシュ関数Hの演算処理が、従来の比較的高速な共通鍵暗号の演算処理と比べても少なくとも数倍以上高速であることから、グループ証明書の発行および検査処理の高速化に寄与するという効果がある。

【0068】

〔第2実施例〕

図17は本発明に基づく第2実施例を示す図（その1）、

図18は同図（その2）である。

この第2実施例でのグループ証明書発行装置3は、クライアント2内に設けられるハッシュ機能部41と協働し、このハッシュ機能部41は前述のテンポラリパスワードtempに対してm回ハッシュ関数Hの演算を適用する。得られた発行側演算値（ハッシュ値）をワンタイムパスワードとなし、前述のグループ証明書GCに代えて、少なくともグループ名およびワンタイムパスワードからなるログイン要求GC'をクライアント2より生成するものである。

【0069】

また第2実施例でのグループ証明書検査部12においては、検査側演算部としてのハッシュ機能部16がテンポラリパスワードtempに対してm回ハッシュ関数Hの演算を適用して検査側演算値（ハッシュ値）をワンタイムパスワードとして再生し、クライアント2側にて同様に生成されたワンタイムパスワードを含むログイン要求GC'より抽出したワンタイムパスワードとが一致することを確認して認証を行う。

【0070】

前述した第1実施例の分散グループ管理システム10では、グループ証明書GCがクライアント2からサーバ1へ送信されるが、このときグループ証明書GCは隠蔽がなされないため、もしこれが盗み見等の原因で漏洩すると、第三者はそのグループ証明書GCをサーバ1へ送信することができる。このとき、サーバ1

にはグループ証明書GCの送信元が正しいユーザであるか第三者であるかを判別することができない。このような攻撃をリプレイ攻撃と呼ぶ。このリプレイ攻撃を防ぐために、第1実施例の分散グループ管理システム10ではグループ証明書蓄積部14にグループ証明書を保持し、これにより二重使用を防いでいる。

#### 【0071】

しかし、そのような二重使用防止策は、正規のユーザが第三者より先にグループ証明書GCをサーバ1へ送信することを前提としており、何らかの理由で正しいユーザがグループ証明書GCを送信する前に、第三者がサーバ1へグループ証明書GCを送信してしまった場合、サーバ1は第三者を正しいと見なし、その後GCを送信してきた正規のユーザは二重使用としてそのリモート処理要求を拒否されてしまう。

#### 【0072】

また、二重使用が拒否されてしまうので、一つのグループ証明書GCは一度しか使うことができない。このため、例えば一度の認証でセッションを確立し、その後の一連のリモート処理要求を1つのセッションとして扱うような場合には構わないが、セッションの概念を用いず、リモート処理要求毎に認証が必要になるような場合には、リモート処理要求のたびに、異なるグループ証明書GCを取得する必要が生じてしまい、効率が悪い。

#### 【0073】

図17および図18を再び参照すると、第1実施例の分散グループ管理システム10においては、前述のとおり、クライアント2からサーバ1へグループ証明書GCが送信されていたが、第2実施例では、これをグループ証明書GCから、暗号的ハッシュ関数Hにより得られるログイン要求GC'に置きかえる。

グループ証明書発行装置3からグループ証明書GCを受け取ったクライアント2は、サーバ1へのリモート処理要求時に、グループ証明書GCの内容のうちテンポラリパスワードtempの値を取り出し、これに通常のワンタイムパスワードと同様の方法でハッシュ関数Hを複数回(m)適用してから、元のテンポラリパスワードと置き換えて、これを変形グループ証明書すなわちログイン要求GC'とする。そして、これをサーバ1へ送信する。

## 【 0 0 7 4 】

サーバ 1 では、グループ証明書（ログイン要求）検査部 1 2 が、グループ秘密情報格納手段 1 3 とグループ証明書（ログイン要求）蓄積部 1 4 とを用いて、ハッシュ関数  $H$  をクライアント 2 と同じ回数だけ適用することで、受け取ったログイン要求  $GC'$  の正当性を検査する。正当であれば、グループ証明書蓄積部 1 4 へログイン要求  $GC'$  とハッシュ関数の適用回数（ $m$ ）に関する情報を格納する。この検査の成功をもって認証機能部 1 1 は認証の完了と見なし、ログイン要求  $GC'$  内のグループ名をグループ権限マッピング格納手段 1 5 にて照合してこのグループに対応する権限を得、クライアント 2 のユーザから要求されるリモート処理の実行に用いる。

## 【 0 0 7 5 】

以上のログイン要求  $GC'$  に関するハッシュ関数  $H$  の適用回数（ $m$ ）を、通常のワンタイムパスワードの手法と同じ要領で、最初は所定の定数回から始め、以後同じグループ証明書を利用してログイン要求を作成または検査するたびに、クライアント 1 およびサーバ 1 のそれぞれで所定の回数（例えば 1）ずつ減じていく。

## 【 0 0 7 6 】

図 1 9 は変形グループ証明書（ログイン要求） $GC'$  の具体的生成方法を示す図である。

変形グループ証明書（ログイン要求） $GC'$  は、グループ証明書  $GC$  内のテンポラリパスワード  $temp$  を種としてワンタイムパスワードを生成することによって作られる。この第 2 実施例では、暗号学的ハッシュ関数  $H$  を複数回（ $m$ ）適用し、回数  $m$  を既定値である  $n$  から同じグループ証明書  $GC$  を用いるたびに 1 ずつ減じていくことによって実現することとする。すなわち、そのグループ証明書  $GC$  を使った今回までの回数を  $k$  として、テンポラリパスワード  $temp$  に（ $n - k$ ）回ハッシュ関数  $H$  を適用し、その結果を、もとのテンポラリパスワードと入れ替えてワンタイムパスワードとすると、これがログイン要求  $GC'$  となる。もし、 $k = n$  に達したら、そのグループ証明書  $GC$  の使用できる回数はそれで終わりであり、発行装置 3 に新たにグループ証明書  $GC$  を発行してもらう必要があ

る。

#### 【0077】

なお、この例では第1実施例でグループ証明書を作成する際に使用したのと同じハッシュ関数Hを用いているが、同じものを用いる必要はない。

図20は第2実施例での変形グループ証明書（ログイン要求）GC'の具体的な検査方法を示す図である。

第1実施例と同様にテンポラリパスワードtemp'を算出したあと、これにハッシュ関数Hをn-k回適用し、予想されるワンタイムパスワードtemp''を生成してから、それをログイン要求GC'の中のワンタイムパスワードtemp'であるべき値と、比較手段20にて比較する。両者が等しければ、受け取ったログイン要求GC'は偽造や改ざん等の施されていない正当なものだと分かる。

#### 【0078】

図21は変形グループ証明書（ログイン要求）蓄積部14内に保持されたデータ例を示す図である。

前記の第1実施例では受け取ったグループ証明書GCをそのまま蓄積部14（図4、図6）に蓄積すればよかったが、第2実施例では同じグループ証明書GC'が使われた回数、すなわち前記のハッシュ関数Hを適用する回数におけるkの値を記憶しておく必要がある。この例では、そのログイン要求GC'が最後に使われたときのkの値を保持している。ただし、0、4、6…はある時点での一例である。

#### 【0079】

図22は第2実施例のもとでの全体の処理の流れを表す図（その1）、

図23は同図（その2）である。

これらの図の処理の流れを、図22および図23を参照しながら説明する。

図22に示す“グループ証明書獲得フェイズ”は、クライアント2が、発行されたグループ証明書を得るまでのプロセスであり、上記の第1実施例と同じであるから説明を省略する。

#### 【0080】

その後、図 2 3 に示すように、サーバ 1 へリモート処理を要求するときに、クライアント 2 はグループ証明書 GC からログイン要求 GC' を前述した方法で生成し、この GC' をサーバ 1 へ送信する。

サーバ 1 は、まず受け取ったログイン要求 GC' を、変形グループ証明書（ログイン要求）検査部 1 2 で検査し、この GC' が正当であれば第 1 実施例と同様にログイン要求 GC' 内のグループ名が正当であるものと見なし、当該グループに与えられた権限の取得を行う（“ログインフェーズ” 参照）。

#### 【 0 0 8 1 】

図 2 4 は変形グループ証明書（ログイン要求）検査部 1 2 の動作の流れを示す図（その 1）、

図 2 5 は同図（その 2）である。

図 2 4 において、まず変形グループ証明書（ログイン要求）蓄積部 1 4 を検索し、有効期限の切れていないログイン要求 GC' のうちで、受け取ったログイン要求 GC' と同じグループ名でかつ同じ有効期限情報を持つものがないか確認する（ステップ S 2 1）。もしなければ、グループ証明書が初めて使われたと見なして  $k = 0$  とし、もしあればその項目の  $k$  の値を取り出し、1 だけ増加させる（ステップ S 2 2, S 2 3 および S 2 4）。

#### 【 0 0 8 2 】

次にこの  $k$  を用いて、図 2 0 に示すとおり、受け取ったログイン要求 GC' を検査し（ステップ S 2 5）、 $temp$  と  $temp'$  が一致すればログイン要求 GC' は正当なものと見なす（ステップ S 2 6 および S 2 7）。このとき、先ほど見つけた検査部 1 2 内の項目を、受け取った新しいログイン要求 GC' とたった今使用した 1 だけ増やした  $k$  の値とで置き換える。さらにその内容を蓄積部 1 4 に格納する（ステップ S 2 9）。

#### 【 0 0 8 3 】

以上述べたとおり、第 2 実施例では、例えばクライアント 2 とサーバ 1 との間の通信が盗み見されるなどして、ログイン要求 GC' が第三者へ漏洩しても、テンポラリーパスワード  $temp$  そのものは漏洩せず、また暗号学的ハッシュ関数  $H$  の性質により、今回漏洩したログイン要求から、次のログイン要求を予測したり算

出したりすることもしない。したがって、サーバ1が同じログイン要求を受け入れない限り、第三者が正当なユーザを偽ってサーバに受け入れられることはなく、正当なユーザはリプレイ攻撃の危険を回避しつつ、1つのグループ証明書GCから複数のログイン要求GC'を作って複数回サーバ1にリモート処理を要求することが可能となる。故に、複数のリモート処理要求を、一度の認証で確立した1セッションとして、受け付けることのできないような場合にも、一度のグループ証明書の発行で済ませることができ、処理効率は大幅に高まる、という効果がある。

【0084】

〔第3実施例〕

図26は本発明に基づく第3実施例を示す図（その1）、

図27は同図（その2）である。

この第3実施例でのグループ証明書発行装置3は、クライアント2内に設けられる一意識別子生成手段42と協働し、この一意識別子生成手段42は、クライアント2とサーバ1との間の相互認証のための認証用識別子auth\_idを生成し、この認証用識別子をグループ証明書GCに含ませてサーバ1に送信するものである。

【0085】

また第3実施例でのグループ証明書検査部12においては、クライアント2とサーバ1との間の相互認証のために、クライアント2より、グループ証明書GCに含ませて送信された認証用識別子auth\_idを受信しこれに対し所定の計算を施してサーバリプライrepを生成し、このサーバリプライはクライアント2に返送され、クライアント2において上記所定の計算と同一の計算を用いて予想されたサーバリプライrep'と比較されて両者が一致したときにクライアント2はそのサーバ1が正当であることを認証可能であるようにする。

【0086】

さらにまた第3実施例でのグループ証明書発行装置3は、送信された認証用識別子auth\_idを含むグループ証明書GCをサーバにおいて受信しこれに対し所定の計算を施して得られたサーバリプライrepをクライアント2に返送し

、その所定の計算と同一の計算を用いてクライアント 2 にて予想したサーバリプライ `rep'` と返送されたサーバリプライ `rep` とを比較して、両者が一致したときに、クライアント 2 は当該サーバが正当であることを認証するようにする。

【0087】

既述した実施例の分散グループ管理システム 10 では、サーバ 1 がクライアント 2 のユーザ `U` を認証しているが、逆にクライアント 2 がサーバを認証することはしていない。すなわち、クライアント 2 がリモート処理を依頼するサーバ 1 が、グループ名に対応したグループの秘密情報 (`secret1`, `secret2` ...) を知っている本物のサーバかどうか、クライアント 2 から確認する手段がない。

【0088】

このため、偽のサーバが偽ってクライアント 2 からの要求を受け付けることを防げないため、セキュリティ上不利がある。

図 26 および図 27 を再び参照すると、第 3 実施例では、既述の実施例の構成要素に加え、クライアント 2 は一意識別子生成手段 42 を有する。

グループ証明書発行装置 3 からグループ証明書 `GC` を受け取ったクライアント 2 は、サーバ 1 へのリモート処理要求時に一意識別子生成手段 42 を用いて、充分な生成回数にわたって一意性があり、なおかつ生成される値が予想できないという性質をもつ認証用識別子 `auth_id` を生成する。そして、この認証用識別子とグループ証明書 `GC` 内のグループ名および有効期限情報 `timestamp` をサーバ 1 へ送信する。

【0089】

これらを受け取ったサーバ 1 は、受け取った三つの値と当該グループに相当する秘密情報とから、これらすべての値を知らなければ生成できないという性質をもつサーバリプライ `rep` の値を、ハッシュ機能部 16 を利用して生成し、この `rep` をクライアント 2 へ返す。

クライアント 2 はテンポラリパスワード `temp` と認証用識別子から予想されるサーバリプライの値を計算し、この値がサーバ 1 から返ってきた前述のサーバリプライ `rep` と等しいかどうか両者を比較する。等しければサーバの認証が成

功したと見なし、その後は既述の実施例と同様にテンポラリパスワード `temp` またはログイン要求 `GC'` をサーバ 1 へ送信して認証を受ける。

#### 【0090】

図 28 はサーバリプライ `rep` の具体的な生成方法を示す図である。

サーバ 1 は、クライアント 2 から受け取ったグループ証明書 `GC`（本図中の最上段）の中から、グループ名および有効期限情報を取り出し、これらに当該グループの秘密情報（`secret 1` とする）を加えてハッシュ関数 `H` を適用し、テンポラリパスワード `temp` を再現する（本図の中段）。

#### 【0091】

さらにそのテンポラリパスワード `temp` に、上記 `GC` から取り出した認証用識別子 `auth_id` を加えて再びハッシュ関数 `H` を適用する。ここに得られた値がサーバリプライ `rep` となる。

図 29 はサーバリプライのクライアント側での具体的検査方法を示す図である。

#### 【0092】

クライアント 2 では、保持していたグループ証明書 `GC` の情報の中からテンポラリパスワード `temp` を取り出し、これに、保持していた前述の認証用識別子 `auth_id` を加えてハッシュ関数 `H` を、サーバ側と同様に適用する。これにより予想されるサーバリプライ `rep'` が得られる。

クライアント 2 は、その `rep'` と、サーバ 1 から返送された図 26 のサーバリプライ `rep` とを、自内の比較手段 43 にて比較し、両者が等しければ、当該サーバは正しいサーバ 1 であることを知ることができる。

#### 【0093】

図 30 は第 3 実施例のもとでの全体の処理の流れを表す図（その 1）、

図 31 は同図（その 2）である。

サーバ 1 へリモート処理を要求するには、クライアント 2 はまず一意識別子生成手段 42 により認証用識別子 `auth_id` を生成し、グループ名、有効期限情報および認証用識別子の 3 つをサーバ 1 へ送信する。サーバ 1 は前述した図 28 に示す方法でサーバリプライ `rep` を生成し、クライアント 2 へ返す。クライ

アント 2 はこれを前述した図 2 9 に示す方法で検査する。もしその検査結果が正しければ、以降は既述の実施例と同様に、グループ証明書 GC あるいはログイン要求 GC' をサーバ 1 へ送信する。

【0094】

なお、認証用識別子 `auth_id` は、次の値を予測することが計算量的に不可能で、ある値が偶然一致してしまうことが確率的にごく少ない程度に一意性を持っている必要がある。単純な乱数でも良いが、偶然一意性を失ってしまうことを避けるために、さらにシリアル番号のように毎回必ず変化する値をその乱数に組み合わせるとなお良い。シリアル番号のみでは次の値が予想できてしまうからである。

【0095】

以上述べたとおり、第 3 実施例では、クライアント 2 が毎回異なる認証用識別子 `auth_id` をサーバ 1 へ送信し、サーバ 1 はその認証用識別子とグループの秘密情報とからサーバリプライ `rep` を生成して、クライアント 2 へ返し、クライアント 2 はこれを検査する。したがって、グループの秘密情報を知らない偽のサーバは、毎回異なる認証用識別子に正しく対応したサーバリプライを生成することができないので、クライアントがサーバを認証することが可能となる。これにより、偽のサーバリモート処理を要求してしまうことを防止でき、安全性が高まる、という効果がある。

【0096】

〔第 4 実施例〕

図 3 2 は本発明に基づく第 4 実施例を示す図（その 1）、

図 3 3 は同図（その 2）である。

この第 4 実施例でのグループ証明書発行装置 3 は、クライアント 2 内に設けられる暗号処理部 4 6 と協働し、この暗号処理部 4 6 は、テンポラリパスワード `temp` を暗号鍵として、クライアント 2 からサーバ 1 への暗号化セッションを確立するように動作する。

【0097】

また第 4 実施例でのグループ証明書検査部 1 2 は、サーバ 1 内に設けられる暗

号処理部 4 5 と協働し、この暗号処理部 4 5 は、テンポラリパスワード `temp` を暗号鍵として、サーバ 1 からクライアント 2 への暗号化セッションを確立するように動作する。

既述した第 1 および第 2 実施例の分散グループ管理システム 1 0 では、サーバ 1 がクライアント 2 のユーザ `U` を認証しているが、逆にクライアント 2 がサーバを認証することはしていない。

#### 【 0 0 9 8 】

このため既述した第 1 および第 2 実施例では、第 3 実施例で述べたようにセキュリティ上の不利がある。

図 3 2 および図 3 3 を再び参照すると、この第 4 実施例では、既述の第 1 および第 2 実施例の構成要素に加え、サーバ 1 とクライアント 2 が同じ暗号アルゴリズムに基づいて暗号化・復号化の処理を行うことができるように、それぞれ暗号処理部 4 5 および 4 6 を有する。

#### 【 0 0 9 9 】

グループ証明書発行装置 3 からグループ証明書 `GC` を受け取ったクライアント 2 は、サーバ 1 へのリモート処理要求時に、グループ名と有効期限情報とをサーバ 1 へ送信する。これらを受け取ったサーバ 1 は、これら 2 つの値とグループの秘密情報とからグループ証明書 `GC` を生成する。以降は、リモート処理要求に関する通信を、グループ証明書内のテンポラリパスワード `temp` の値を暗号鍵として暗号化し、互いに送信して、受信したら復号化する。

#### 【 0 1 0 0 】

図 3 4 は第 4 実施例のもとでの全体の処理の流れを表す図である。ただし、“グループ証明書獲得フェーズ”は前述したのと同様であるので“ログインフェーズ”のみを示す。

第 4 実施例では、第 1 および第 2 実施例と同様に、グループ証明書 `GC` の発行を受けたあと、クライアント 2 はグループ名および有効期限情報 `timestamp` を送信し、サーバ 1 は、これらとグループの秘密情報とからテンポラリパスワード `temp` を計算する。これにより、テンポラリパスワードの値がサーバ 1 とクライアント 2 との間で共有されるので、以降この値を暗号鍵として暗号通信

を行うことにより、第 3 実施例の場合のように明示的に認証をしなくとも、正しい相手に対してのみ、通信内容を送ることができる。図 3 4 のログインフェイズの処理の流れの例では、クライアント 2 からセッション識別子 `session-id` を送信しているが、これは同じサーバに複数のユーザ U やクライアント 2 が接続した場合に、サーバ側でそれらを区別するために追加されているものである。したがって第 4 実施例の原理には必ずしも必要でない。セッション識別子 `session-id` は、クライアント 2 で明示的に生成して送信してもよいし、あるいは通信手段等から得られる値、例えばクライアントのホストアドレスやポート番号などを用いても構わない。

#### 【0101】

以上述べたとおり、第 4 実施例では、クライアント 2 は発行されたグループ証明書 GC から、そしてサーバ 1 はクライアント 2 から受け取ったグループ名、有効期限情報および自身が保持するグループの秘密情報の 3 つから、それぞれ、テンポラリパスワード `temp` を得て秘密裏に該 `temp` を共有することができる。

#### 【0102】

このテンポラリパスワード `temp` により、以降の通信を暗号化して行えば、この暗号化された通信を復号化できるのは上記の両者のみ（グループ証明書発行装置 3 は除く）であるから、明示的に認証をしなくとも、あたかも相互に認証したのと同様に、正しい相手にしか通信内容は伝わらない。これにより、偽のサーバヘリモート処理を要求してしまうことを防止でき、安全性が高まる、という効果がある。

#### 【0103】

##### 〔第 5 実施例〕

図 3 5 は本発明に基づく第 5 実施例を示す図（その 1）、

図 3 6 は同図（その 2）である。

この第 5 実施例でのグループ証明書発行装置 3 は、ユーザ U の各々について各リモート処理要求にかかるセッションの履歴を記録するログファイル 4 8 を備え、その履歴をもとに各ユーザの監査を行うようにするものである。

## 【 0 1 0 4 】

また第 5 実施例でのグループ証明書検査部 1 2 は、サーバ 1 内に設けられるログファイル 4 7 と協働し、このログファイル 4 7 は、ユーザ U の各々について各リモート処理要求にかかるセッションの履歴を記録し、この履歴をもとに各ユーザの監査を行うようにするものである。

さらにまた、第 5 実施例のグループ証明書発行装置 3 において、上記の履歴にはそれぞれセッション毎のテンポラリパスワード t e m p を含ませ、各セッションを識別するようにする。

## 【 0 1 0 5 】

また第 5 実施例のグループ証明書検査部 3 は、上記の履歴にそれぞれセッション毎のテンポラリパスワード t e m p を含ませ、各セッションを識別可能とする。

サーバにおいては、誰がどのような動作を要求し何が行われたか、をログに記録することがしばしば行われる。ところが既述の実施例の分散グループ管理システム 1 0 では、サーバ 1 はどのグループに基づいての要求かは知ることができるが、実際にどのユーザがその要求を送信してきたのかは知ることができない。このため、たとえば一部の処理についてユーザごとに課金したり、また重要な処理について違反が行われたり、といった特別な場合に、ログからどのユーザがその処理に関係しているのか知ることができないという不利がある。

## 【 0 1 0 6 】

第 5 実施例のシステム 1 0 では、第 1 実施例のシステムに加え、サーバ 1 はログファイル 4 7 を有し、グループ証明書発行装置 3 はログファイル 4 8 を有する。

グループ証明書発行装置 3 のグループ証明書発行部 3 1 は、第 1 実施例で述べたグループ証明書発行の処理を行う際に、ユーザ名およびグループ証明書を一意に識別できる情報（例えばテンポラリパスワード t e m p ）を、ログとして通常記録されるべき他の情報（例えばサーバ名、発行日時、有効期限情報等）と共に、ログファイル 4 8 へ記録する。

## 【 0 1 0 7 】

サーバ 1 の認証機能部 1 1 は、第 1 実施例で述べたグループ証明書 G C を受け取り、あるいは検査を行う際に、グループ名およびそのグループ証明書と同じグループ証明書を一意に識別できる情報を、ログとして通常記録されるべき他の情報と共に、ログファイル 4 7 へ記録する。なお、以上の本実施例の説明は第 1 実施例のシステム 1 0 に対する改良として述べたが、その他の実施例のシステムに対しても同様の改良が可能である。また、前記の「一意に識別できる情報」とは、情報理論的（絶対的）に完全に一意でなくとも、確率的に一意と見なせれば十分である。

#### 【 0 1 0 8 】

図 3 7 は第 5 実施例のグループ証明書発行装置 3 におけるログファイル 4 8 内のデータの一例を示す図であり、

図 3 8 は第 5 実施例のサーバ 1 におけるログファイル 4 7 内のデータの一例を示す図である。

前述のとおり第 5 実施例は、既述の実施例に加えて、グループ証明書発行装置 3 とサーバ 1 がそれぞれログをログファイル 4 8, 4 7 に記録しており、これらを照合することによって、ユーザごとの監査が可能になる。

#### 【 0 1 0 9 】

図 3 7 を参照すると、ユーザとそのユーザに発行されたグループ証明書 G C を特定するためには、ユーザ名とテンポラリパスワード `temp` があれば充分であるが、この例ではその他に発行日時、サーバ名、グループ名および発行したグループ証明書 G C の有効期限情報 (`timestamp`) がログファイル 4 8 に記録されている。

#### 【 0 1 1 0 】

図 3 8 を参照すると、上記グループ証明書発行装置 3 内のログファイル 4 8 の場合と同様に、グループ証明書を特定するためのテンポラリパスワード `temp` に加え、リモート処理の開始日時と終了日時、クライアントのホスト名、グループ名および有効期限情報がログファイル 4 7 に記録されている。

サーバ 1 がログファイル 4 7 にどんな事象を記録するか、いつ何を契機として記録するか、は本発明では特に限定しないが、例えば、グループ証明書を受け取

ったとき、グループ証明書の検査が成功したとき、課金が必要であるような重要なりモート処理が行われたとき、セキュリティやリモート処理の実行に重大な違反が生じたとき等を挙げることができる。

#### 【0111】

なお、これらの例ではテンポラリパスワードは10進数字の羅列として表現されているが、元のテンポラリパスワードを一意に判別できるような形式であれば、どのような形式でログファイル47、48に記録してもよい。

以上述べたとおり、第5実施例では、サーバ1側のログファイル47にはグループ証明書GCを一意に識別できる情報とグループ名とを含んだログが記録されており、一方、グループ証明書発行装置3側のログファイル48にはグループ証明書GCを一意に識別できる情報とユーザ名とを含んだログが記録されている。換言すれば、サーバ1側のログファイル48にはどのグループ証明書を用いて何が要求され何が行われたか、が記録されており、一方、グループ証明書発行装置3側のログファイル47には、どのグループ証明書をどのユーザへ発行したかが記録されている。

#### 【0112】

したがって、両者のログファイルを、グループ証明書を、一意に識別できる情報が同じである項目同士で照合することによって、どのユーザがサーバに何を要求し何を行ったかを知ることができる、という効果がある。

#### 〔第6実施例〕

図39は本発明に基づく第6実施例を示す図（その1）、

図40は同図（その2）である。

#### 【0113】

この第6実施例でのグループ証明書発行装置3は、一意識別子生成手段51をさらに含むと共に、発行側演算部をなすハッシュ機能部34は、グループ名およびそのグループに固有の秘密情報にさらに有効期限情報（*timestamp*）を加えてハッシュ関数Hの演算を適用し、得られた発行側演算値（ハッシュ値）をテンポラリパスワード（*temp*）となし、グループ名、有効期限情報（*timestamp*）およびそのテンポラリパスワードからグループ証明書GCを生

成する。ここに一意識別子生成手段 5 1 は、同一内容のグループ証明書 G C が、複数の異なるユーザに対して発行されるとき、これらのグループ証明書をこれらのユーザ毎に識別する証明書識別子を生成して対応する各グループ証明書 G C に付加するようにしたものである。

【 0 1 1 4 】

また第 6 実施例でのグループ証明書検査部 1 2 は、同一内容のグループ証明書 G C が、複数の異なるユーザに対して発行されるとき、これらのグループ証明書をこれらのユーザ毎に識別する証明書識別子が付加された各グループ証明書 G C をクライアント 2 から受信し、これらの証明書識別子により、複数の異なるユーザを同一のグループに割り当てるようにしたものである。

【 0 1 1 5 】

同様にこの第 6 実施例でのグループ証明書発行装置 3 は、上述の一意識別子生成手段 5 1 を同様に含むと共に、発行側演算部をなすハッシュ機能部 3 4 は、グループ名およびそのグループに固有の秘密情報にさらに有効期限情報を加えてハッシュ関数 H の演算を適用し、得られたテンポラリパスワード  $t_{emp}$  をもとにワンタイムパスワード  $t_{emp}'$  を得て、ログイン要求 G C' を生成する。ここに一意識別子生成手段 5 1 は、同一内容のログイン要求 G C' が、複数の異なるユーザに対して発行されるとき、これらのログイン要求をこれらのユーザ毎に識別する証明書識別子を生成して対応する各ログイン要求 G C' に付加するようにしたものである。

【 0 1 1 6 】

上記のグループ証明書発行装置 3 に対応させたグループ証明書検査部 1 2 は、同一内容のログイン要求 G C' が、複数の異なるユーザに対して発行されるときこれらのログイン要求をこれらのユーザ毎に識別するログイン要求識別子が付加された各ログイン要求 G C' をクライアント 2 から受信し、これらのログイン要求識別子により、複数の異なるユーザを同一のグループに割り当てるようにしたものである。

【 0 1 1 7 】

既述の実施例での分散グループ管理システム 1 0 では、同一のグループ証明書

が重複して発行されることがあり得る。すなわち、複数のユーザが、同一または別個のクライアント 2 から、同じサーバの同じグループに対する同じ有効期限を有するグループ証明書 GC の発行を、グループ証明書発行装置 3 に求めたとしても、異なるユーザに対して同じ内容のグループ証明書が発行されることになる。なぜなら、グループ証明書 GC は、グループ名、有効期限情報 ( t i m e s t a m p ) およびテンポラリパスワード ( t e m p ) からなり、このテンポラリパスワードは、グループ名、有効期限情報およびグループの秘密情報から一意に作成されるものだからである。

## 【 0 1 1 8 】

したがって、複数の異なるユーザを、グループ証明書 GC によってあるいはその GC から生成されたログイン要求 GC' によっては区別することができない、という不都合が生じる。例えば、第 1 実施例ではサーバ 1 は同じグループ証明書の二重使用を拒否してしまうため（不正使用防止のため）、一方のユーザが先にグループ証明書を使用して一旦サーバ 1 を利用してしまうと、そのあとの他のユーザによる利用は拒否されてしまい、サーバ 1 を利用するには新たにグループ証明書あるいはログイン要求発行を受けねばならない。これはシステム 1 0 を非効率的なものにしてしまう、という不利が生ずる。

## 【 0 1 1 9 】

第 6 実施例の分散グループ管理システム 1 0 は、既述の実施例のシステムに加え、グループ証明書 GC あるいはログイン要求 GC' に、証明書識別子を付与する機能を備える。この証明書識別子は、グループ証明書 GC が重複して発行される頻度の範囲ならば、充分に一意性を有するものである。この場合、証明書識別子の生成方法としては、例えば、乱数またはシリアル番号などの使用が挙げられる。

## 【 0 1 2 0 】

グループ証明書発行装置 3 は、そのための一意識別子生成手段 5 1 を有し、グループ証明書 GC を発行するときに該手段 5 1 を用いてグループ証明書 GC （あるいは GC' ）を一意に識別できる証明書識別子を生成し、これをグループ証明書 GC （あるいは GC' ）に付与して発行する。

クライアント 2 は、グループ証明書 G C 内の証明書識別子を、グループ名や有効期限情報と同様に取り扱う。ログイン要求 G C' を生成する場合には、グループ名や有効期限情報と同様に、そのログイン要求に証明書識別子を付与する。

#### 【 0 1 2 1 】

サーバ 1 は証明書識別子を、グループ名や有効期限情報と同様に、グループ証明書あるいはログイン要求を構成する値として取り扱い、識別、検査、格納に利用する。

図 4 1 は第 6 実施例に基づく証明書識別子 C i d の一例を示す図である。

第 6 実施例では、一例として、有効期限情報に、一意性のある証明書識別子 C i d を加えることによって、同じサーバ名／グループ名／有効期限情報から、異なるグループ証明書 G C を異なるユーザに対して発行することを可能にしている。

#### 【 0 1 2 2 】

図 4 1 を参照すると、有効期限情報に証明書識別子を加える場合を示しており、ここでは一例としてグループ証明書 G C を作成する際に、ハッシュ関数 H を適用する前のデータ構造に付与する場合を示している。本図のように、有効期限の日時のあとに 8 桁 1 0 進整数の証明書識別子 C i d を付け加えている。この証明書識別子 C i d はグループ証明書発行装置 3 毎に（装置 3 が複数あるとき）、またグループ証明書を発行するたびに、1 ずつ増加されるシリアル番号である。

#### 【 0 1 2 3 】

なお既に生成済みの有効期限情報の日時と証明書識別子とを、図 4 1 に示すように、まとめて取り出して扱えば、既述の各実施例の場合と同様に G C を扱うことができる、というメリットが生まれるが、本図の右に示すように、C i d を個別に扱っても構わない。

以上述べたとおり、第 6 実施例では、グループ証明書 G C またはログイン要求 G C' に、一意な証明書識別子 C i d を付与することにより、例え同じサーバの同じグループに対する同じ有効期限を持ったグループ証明書が複数の異なるユーザにそれぞれ発行されても、これらを区別することができ、グループ証明書あるいはログイン要求の重複が回避される。

## 【 0 1 2 4 】

これにより、例え異なるユーザが重複したグループ証明書の発行を要求したとしても、各ユーザ毎に異なるグループ証明書が発行される。したがって、前述したごとく、二重使用の拒否のために、二度目以降に使用しようとした他のユーザによるリモート処理要求が、サーバ 1 から拒否されるといった不都合は解消されるので、該他のユーザは新たなグループ証明書の発行を受けずに済むから、システムの効率が高まる、という効果が生じる。

## 【 0 1 2 5 】

## 〔第 7 実施例〕

図 4 2 は本発明に基づく第 7 実施例を示す図（その 1）、

図 4 3 は同図（その 2）である。

この第 7 実施例でのグループ証明書発行装置 3 は、ユーザーグループマッピング格納手段 3 2 を備え、このユーザーグループマッピング格納手段において、一人のユーザについて複数の異なるグループを割り当て可能としたものである。

## 【 0 1 2 6 】

また第 7 実施例でのグループ証明書検査部 1 2 は、サーバ 1 内に設けられるグループ証明書一時蓄積部 5 2 と協働し、一人のユーザ U について複数の異なるグループを割り当て可能とするとき、クライアント 2 から受信したグループ証明書 GC を検査したあとこれをそのグループ証明書一時蓄積部 5 2 に蓄積する。そして以降のリモート処理要求に対し、その要求に必要な所定の権限に応じて、その蓄積されたグループ証明書 GC を切り替えて使用するようにしたものである。

## 【 0 1 2 7 】

同様にこの第 7 実施例でのグループ証明書検査部 1 2 は、サーバ 1 内に設けられるログイン要求一時蓄積部 5 2 と協働し、一人のユーザ U について複数の異なるグループを割り当て可能とするとき、クライアント 2 から受信したログイン要求 GC' を検査したあとこれをそのログイン要求一時蓄積部 5 2 に蓄積する。そして以降のリモート処理要求に対し、その要求に必要な所定の権限に応じて、その蓄積されたログイン要求を切り替えて使用するようにしたものである。

## 【 0 1 2 8 】

既述した実施例の分散グループ管理システム 10 では、1 人のユーザ U に対して複数のグループ名が割り当てられていた場合に、クライアント 2 から、希望するグループ名を指定する仕組みを追加するなどして、容易にクライアント 2 のユーザ U が複数のグループ名にそれぞれ対する複数のグループ証明書 GC を得るように変更することができる。

#### 【0129】

ところが、最終的に、グループに割り当てられた権限を知って判断をするのはサーバ 1 であり、ユーザ U は、自分が依頼したいリモート処理の実行に適切な権限が割り当てられたグループ名を、正しく選択できるとは限らない。したがって、いくつかのグループ証明書 GC あるいはログイン要求 GC' を順にサーバ 1 へ送ることで試行錯誤的にリモート処理を要求しなければならず、不便で非効率的な作業を必要とする、という不利がある。

#### 【0130】

また、例えユーザが必要なグループを知っていて、正しくグループを選択できたとしても、一連の関連したリモート処理に要する権限が、複数の異なるグループ名を必要とする場合において、次のグループ名に処理を移行しなければならないとき、現在割り当てられているグループ名では権限がないといった場合には、その権限がないことをサーバ 1 から通知される。このためそのユーザは、改めて新たなグループのメンバーとしてリモート処理の要求をしなければならず、システム 10 が不便かつ非効率的なものになる、という不利がある。

#### 【0131】

図 4 2 および図 4 3 を再び参照すると、第 7 実施例の分散グループ管理システム 10 は、既述した実施例のシステムに加え、サーバ 1 にグループ証明書一時蓄積部 5 1 を有する。クライアント 2 が複数のグループ証明書 GC 1 … GC k をサーバ 1 へ送信した場合に、サーバ 1 がそれらの GC を 1 つ 1 つ検査した上で、グループ証明書一時蓄積部 5 2 へ格納しておく。これにより、クライアント 2 がグループ証明書を選択したり、サーバ 1 がクライアント 2 に、必要なグループ証明書の送信を問い合わせたりしなくとも、サーバ 1 自身が、必要なグループ証明書を、グループ証明書一時蓄積部 5 2 から取り出して利用できる。

## 【0132】

グループ証明書発行装置3から複数のグループ証明書GC1…GCkを受け取ったクライアント2は、サーバ1へのリモート処理を要求するときに、これら複数のグループ証明書をサーバ1へ送信する。

これらGC1…GCkを受け取ったサーバ1は、受け取った複数のグループ証明書の1つ1つを、既述の実施例の場合と同様に検査する。この場合、複数のグループ証明書のうちの一部が不正であった場合の取扱いについて本発明では特に規定しないが、例えばすべてのグループ証明書を拒否するとか、不正なもののみ拒否し正当なものだけを受け付けて処理を進める、等の対処が挙げられる。

## 【0133】

上記の検査の結果、正当であったグループ証明書は、有効期限（time stamp）が切れるか、あるいは別途定められた期間が過ぎるまで、グループ証明書一時蓄積部52に蓄積しておく。それ以降は、サーバ1はユーザUの要求するリモート処理に応じて、適切なグループ証明書をグループ証明書一時蓄積部52から切り替えて取り出し、既述の実施例の場合と同様にこれを利用する。

## 【0134】

なお、グループ証明書GCではなくログイン要求GC'をサーバ1へ送る場合には、グループ証明書の代わりにログイン要求について上記と同様の処理を行う。

図44は第7実施例に基づくユーザーグループマッピング格納手段32内のデータの一例を示す図である。

## 【0135】

上述のとおり、第7実施例は、1人のユーザUに複数のグループ名が割り当てられていて、それら複数のグループ名に対するグループ証明書GCが発行される場合において、クライアント2がグループ証明書GCを選んで送信するのではなく、複数のグループ証明書をサーバ1へ送信しておき、サーバ1側でこれらをグループ証明書一時蓄積部52に一時的に蓄積しておくことで、クライアント2が選択したりサーバ1からクライアント2に別のグループ証明書を要求しなくとも、サーバ1が必要なグループを選択して利用できるようにするものであり、この

ために、1人のユーザに複数のグループ名が割り当てられている場合、図41に示すとおり、格納手段32内に、各ユーザ毎に、複数のグループ名を格納しておく。

#### 【0136】

なお、本図の右側のグループの欄では、サーバ名（server X, Y等）は省略した。これらサーバ名は、同図左側のユーザの欄に示したものと全く同じである。

図45は第7実施例で採用するグループ証明書一時蓄積部52内のデータの一例を示す図である。

#### 【0137】

本図において、この蓄積部52内には、サーバ1内で既に検査を受けて正当とされた複数のグループ証明書GCが格納されている。この例ではセッション識別子Sid（例えば7桁の数字）と一緒に格納されている。これは、1つのサーバに複数のユーザが接続する際に、それらを区別するためにつけた識別子であるが、本実施例の原理からすると、必ずしも必要でない。このセッション識別子Sidは、クライアント2から明示的に申告させてもよいし、あるいは通信手段から得られる情報、たとえばクライアントのホストアドレスやポート番号を用いてその識別子としてもよい。

#### 【0138】

図46は第7実施例のもとでの全体の処理の流れを表す図（その1）、

図47は同図（その2）である。ただし“グループ証明書獲得フェーズ”（例えば図23参照）は記載を省略し、それ以降の“ログインフェーズ”について詳しく示す。

まず図46において、複数のグループ証明書GC1～GC3が発行され、クライアント2がそれらを得るまでは既述の実施例の場合と同様であり、その後、クライアント2がサーバ1へリモート処理を要求する際に、クライアント2は発行された上記複数のグループ証明書をサーバ1へ送信する。

#### 【0139】

上記複数のグループ証明書を受け取ったサーバ1は、既述の実施例の場合と同

様に、グループ証明書検査部 1 2 においてそれぞれの正当性を検査する。この検査の結果をどのように扱うかという処置については、いくつか考えられるが、本発明では特に規定しない。

検査済みのグループ証明書はグループ証明書一時蓄積部 5 2 へ格納しておき、以降のリモート処理において必要とされるいずれかのグループ証明書を適宜選んで利用する。以下に、グループ証明書をサーバが適宜選択する例を示すが、ここでは、第 1 実施例の図 1 1 に示したグループ権限マッピング格納手段 1 5 のデータを例にとって説明する。

#### 【0 1 4 0】

ユーザ `user B` は、図 4 4 に従い、`group 1`、`group 2`、`group 3` の 3 つのグループに対する各グループ証明書を受け取り、図 4 7 に示すごとく、それらをサーバ 1 へ送信する。サーバ 1 は上記 3 つのグループ証明書を検査して、検査の結果いずれも正当と判断したとする。このあと、ユーザ `user B` は「`file A` を読み出し (r)、その結果を `file B` へ書き込む (w)」(図 1 1 参照) というリモート処理を要求したとする。この場合、`file A` の読み出し (r) については `group 1` の権限で充分であったので、サーバ 1 はグループ証明書一時蓄積部 5 2 から `group 1` に対応するグループ証明書 GC を取り出し、この GC をグループ権限マッピング格納手段 1 5 での照合に用いる。なお、第 5 実施例のようにログを取る必要があれば、`group 1` に対応するグループ証明書を用いて、ログファイル 4 7 (図 3 6) に記録する。

#### 【0 1 4 1】

次に上記の読み出し (r) の結果を `file B` へ書き込む (w) が、これには `group 1` の権限 (r のみ) では不充分であり、`group 3` の権限 (r と w の双方) が必要である。したがってサーバ 1 はグループ証明書一時蓄積部 5 2 から `group 3` に対応するグループ証明書 GC 3 に切り替えてこれを取り出し、この GC 3 を手段 1 5 での照合に用いて対応する権限 (r と w) を得る。もし必要なら、`group 3` に対応するグループ証明書 GC 3 を用いてログファイル 4 7 に記載して、`file B` へ書き込みを行う。

#### 【0 1 4 2】

以上述べたとおり、第 7 実施例では、クライアント 2 から送信された複数のグループ証明書 GC あるいはログイン要求 GC' を、サーバ 1 が検査したあと一時的に蓄積しておくので、ユーザ U の要求するリモート処理に応じて、それらの中から適宜選択して利用する。

これにより、ユーザ U がリモート処理に必要なグループメンバシップを知らない場合や、また、一連のリモート処理に複数の異なるグループメンバシップが必要な場合であっても、サーバ側で適切なグループ証明書あるいはログイン要求を適宜切り替えながら選択して処理を進めることができるため、ユーザ側では一度複数のグループ証明書あるいはログイン要求を送信するだけでよいことになり、システム 10 の利便性と効率が高まる、という効果が得られる。

#### 【0143】

以上述べた本発明の実施の態様は以下の付記のとおりである。

(付記 1) ユーザ側のクライアントと、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバとに対してセキュリティ管理を行うために、ユーザのグループへの所属を間接的に認証する分散グループ管理システムにおいて、

前記リモート処理要求があったとき、当該ユーザが所属するグループ名を含む原グループ情報をもとにグループ証明書をクライアント側で発行するグループ証明書発行装置と、

クライアント側から送信された前記グループ証明書の正当性を前記サーバ内にて検査するグループ証明書検査部と、を備え、

ここに前記グループ証明書発行装置は、該原グループ情報の情報を暗号学的関数により演算した発行側演算値を該原グループ情報に付加して該グループ証明書とし、

前記グループ証明書検査部は、受信した前記グループ証明書に含まれる一部の情報を同一の前記暗号学的関数により演算して検査側演算値を得、前記発行側演算値と前記検査側演算値とが一致することを確認して前記の認証を行うことを特徴とする分散グループ管理システム。

#### 【0144】

（付記 2）前記グループ証明書発行装置は、前記グループに割り当てた秘密情報を前記原グループ情報に含ませて前記暗号学的関数による演算を行い、

前記グループ証明書検査部は、前記グループに割り当てた秘密情報を、受信した前記グループ証明書に含まれる一部の情報に含ませて前記暗号学的関数による演算を行い、

前記グループ証明書発行装置および前記サーバは、同一のグループについて同一の前記秘密情報を相互に共有することを特徴とする付記 1 に記載の分散グループ管理システム。

【 0 1 4 5 】

（付記 3）前記暗号学的関数が、ハッシュ関数であることを特徴とする付記 1 に記載の分散グループ管理システム。

（付記 4）ユーザ側のクライアントと、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバとに対してセキュリティ管理を行うために、ユーザのグループへの所属を間接的に認証する分散グループ管理方法において、

クライアント側で、前記リモート処理要求があったとき、当該ユーザが所属するグループ名を含む原グループ情報の情報を暗号学的関数により演算し、得られた発行側演算値を該原グループ情報に付加したグループ証明書を発行する第 1 ステップと、

サーバ側で、受信した前記グループ証明書の情報を同一の前記暗号学的関数により演算して検査側演算値を得る第 2 ステップと、

サーバ側で、前記検査側演算値と受信した前記発行側演算値とを比較し、これらが一致することを確認することにより前記の認証を行い、クライアント側から送信された前記グループ証明書の正当性を前記サーバ内にて検査する第 3 ステップと、を有することを特徴とする分散グループ管理方法。

【 0 1 4 6 】

（付記 5）ユーザ側のクライアントと、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバとに対してセキュリティ管理を行うために、ユーザのグループへの所属を間接的に認証する分散

グループ管理システムを構成するグループ証明書発行装置であって、

前記リモート処理要求があったとき、当該ユーザが所属するグループ名を含む原グループ情報を発行すると共に、該原グループ情報の情報を暗号学的関数により演算した発行側演算値を該原グループ情報に付加して該グループ証明書とする発行側演算部を備えることを特徴とするグループ証明書発行装置。

【0147】

（付記6）ユーザ側のクライアントと、各グループ毎に割り当てられた所定の権限のもとにユーザ側からのリモート処理要求を実行するサーバとに対してセキュリティ管理を行うために、ユーザのグループへの所属を間接的に認証する分散グループ管理システムを構成するグループ証明書検査部であって、

前記サーバ側において、クライアント側から受信したグループ証明書に含まれる情報を、暗号学的関数により演算して検査側演算値を生成する検査側演算部を含み、その受信したグループ証明書に含まれる発行側演算値と前記検査側演算値とが一致することを確認して前記の認証を行うことを特徴とするグループ証明書検査部。

【0148】

（付記7）前記暗号学的関数がハッシュ関数であって、前記発行側演算部は該ハッシュ関数の演算を行うハッシュ機能を備えることを特徴とする付記5に記載のグループ証明書発行装置。

（付記8）前記発行側演算部は、少なくともグループ名およびそのグループに固有の秘密情報に対し一括して前記ハッシュ関数の演算を適用し、得られた前記発行側演算値をテンポラリパスワードとなし、少なくとも前記グループ名および前記テンポラリパスワードから前記グループ証明書を生成することを特徴とする付記7に記載のグループ証明書発行装置。

【0149】

（付記9）前記クライアント内に設けられるハッシュ機能部と協働し、該ハッシュ機能部は前記テンポラリパスワードに対してm回前記ハッシュ関数の演算を適用し、得られた前記発行側演算値をワンタイムパスワードとなし、前記グループ証明書に代えて、少なくとも前記グループ名および前記ワンタイムパスワード

からなるログイン要求を該クライアントより生成することを特徴とする付記 8 に記載のクライアント。

【0150】

(付記 1 0) 前記クライアント内に設けられる一意識別子生成手段と協働し、該一意識別子生成手段は、前記クライアントと前記サーバとの間の相互認証のための認証用識別子を生成し、該認証用識別子を前記グループ証明書に含ませて前記サーバに送信することを特徴とする付記 8 に記載のグループ証明書発行装置。

(付記 1 1) 送信された前記認証用識別子を含む前記グループ証明書を前記サーバにおいて受信しこれに対し所定の計算を施して得られたサーバリプライを前記クライアントに返送し、該所定の計算と同一の計算を用いて該クライアントにて予想したサーバリプライと返送されたサーバリプライとを比較して、両者が一致したときに該クライアントは該サーバが正当であることを認証することを特徴とする付記 1 0 に記載のグループ証明書発行装置。

【0151】

(付記 1 2) 前記クライアント内に設けられる暗号処理部と協働し、該暗号処理部は、前記テンポラリパスワードを暗号鍵として、該クライアントから前記サーバへの暗号化セッションを確立することを特徴とする付記 8 に記載のグループ証明書発行装置。

(付記 1 3) 前記ユーザの各々について各前記リモート処理要求にかかるセッションの履歴を記録するログファイルを備え、該履歴をもとに各該ユーザの監査を行うことを特徴とする付記 8 に記載のグループ証明書発行装置。

【0152】

(付記 1 4) 前記履歴にはそれぞれ前記セッション毎の前記テンポラリパスワードを含ませ、各該セッションを識別することを特徴とする付記 1 3 に記載のグループ証明書発行装置。

(付記 1 5) 一意識別子生成手段をさらに含むと共に、

前記発行側演算部は、前記グループ名およびそのグループに固有の秘密情報にさらに有効期限情報を加えて前記ハッシュ関数の演算を適用し、得られた前記発行側演算値をテンポラリパスワードとなし、前記グループ名、前記有効期限情報

および前記テンポラリパスワードから前記グループ証明書を生成し、

前記一意識別子生成手段は、同一内容の該グループ証明書が、複数の異なる前記ユーザに対して発行されるとき、これらのグループ証明書をこれらのユーザ毎に識別する証明書識別子を生成して対応する各該グループ証明書に付加することを特徴とする付記 8 に記載のグループ証明書発行装置。

【 0 1 5 3 】

(付記 1 6) 一意識別子生成手段をさらに含むと共に、

前記発行側演算部は、前記グループ名およびそのグループに固有の秘密情報にさらに有効期限情報を加えて前記ハッシュ関数の演算を適用し、得られた前記テンポラリパスワードをもとに前記ワンタイムパスワードを得て、前記ログイン要求を生成し、

前記一意識別子生成手段は、同一内容の該ログイン要求が、複数の異なる前記ユーザに対して発行されるとき、これらのログイン要求をこれらのユーザ毎に識別する証明書識別子を生成して対応する各該ログイン要求に付加することを特徴とする付記 9 に記載のグループ証明書発行装置。

【 0 1 5 4 】

(付記 1 7) ユーザーグループマッピング格納手段を備え、該ユーザーグループマッピング格納手段において、一人の前記ユーザについて複数の異なるグループを割り当て可能であることを特徴とする付記 7 に記載のグループ証明書発行装置。

(付記 1 8) 前記暗号学的関数がハッシュ関数であって、前記検査側演算部は該ハッシュ関数の演算を行うハッシュ機能を備えることを特徴とする付記 6 に記載のグループ証明書検査部。

【 0 1 5 5 】

(付記 1 9) 前記検査側演算部は、クライアント側から受信した前記グループ証明書に少なくとも含まれるグループ名およびそのグループに固有の秘密情報に対し一括して前記ハッシュ関数の演算を適用することにより前記検査側演算値を、再現されたテンポラリパスワードとして再生することを特徴とする付記 1 8 に記載のグループ証明書検査部。

## 【 0 1 5 6 】

（付記 2 0）前記検査側演算部はハッシュ機能部であり、該ハッシュ機能部は前記テンポラリパスワードに対して m 回前記ハッシュ関数の演算を適用して前記検査側演算値をワンタイムパスワードとして再生し、クライアント側にて同様に生成されたワンタイムパスワードを含むログイン要求より抽出した該ワンタイムパスワードとが一致することを確認して前記の認証を行うことを特徴とする付記 1 9 に記載のグループ証明書検査部。

## 【 0 1 5 7 】

（付記 2 1）前記クライアントと前記サーバとの間の相互認証のために、該クライアントより、前記グループ証明書に含ませて送信された認証用識別子を受信しこれに対し所定の計算を施してサーバリプライを生成し、該サーバリプライは前記クライアントに返送され、該クライアントにおいて該所定の計算と同一の計算を用いて予想されたサーバリプライと比較されて両者が一致したときに該クライアントは該サーバが正当であることを認証可能であることを特徴とする付記 1 9 に記載のグループ証明書検査部。

## 【 0 1 5 8 】

（付記 2 2）前記サーバ内に設けられる暗号処理部と協働し、該暗号処理部は、前記テンポラリパスワードを暗号鍵として、該サーバから前記クライアントへの暗号化セッションを確立することを特徴とする付記 1 9 に記載のグループ証明書検査部。

（付記 2 3）前記サーバ内に設けられるログファイルと協働し、該ログファイルは、前記ユーザの各々について各前記リモート処理要求にかかるセッションの履歴を記録し、該履歴をもとに各該ユーザの監査を行うことを特徴とする付記 1 8 に記載のグループ証明書検査部。

## 【 0 1 5 9 】

（付記 2 4）前記履歴にはそれぞれ前記セッション毎の前記テンポラリパスワードを含ませ、各該セッションを識別することを特徴とする付記 2 3 に記載のグループ証明書検査部。

（付記 2 5）同一内容の前記グループ証明書が、複数の異なる前記ユーザに対

して発行されるとき、これらのグループ証明書をこれらのユーザ毎に識別する証明書識別子が付加された各該グループ証明書を前記クライアントから受信し、該証明書識別子により、前記複数の異なるユーザを同一の前記グループに割り当てることを特徴とする付記 1 9 に記載のグループ証明書検査部。

#### 【0160】

（付記 2 6）同一内容の前記ログイン要求が、複数の異なる前記ユーザに対して発行されるときこれらのログイン要求をこれらのユーザ毎に識別するログイン要求識別子が付加された各該ログイン要求を前記クライアントから受信し、該ログイン要求識別子により、前記複数の異なるユーザを同一の前記グループに割り当てることを特徴とする付記 2 0 に記載のグループ証明書検査部。

#### 【0161】

（付記 2 7）前記サーバ内に設けられるグループ証明書一時蓄積部と協働し、一人の前記ユーザについて複数の異なるグループを割り当て可能とするとき、前記クライアントから受信した前記グループ証明書を検査したあとこれを該グループ証明書一時蓄積部に蓄積し、以降の前記リモート処理要求に対し、その要求に必要な前記所定の権限に応じて、その蓄積された該グループ証明書を切り替えて使用することを特徴とする付記 1 8 に記載のグループ証明書検査部。

#### 【0162】

（付記 2 8）前記サーバ内に設けられるログイン要求一時蓄積部と協働し、一人の前記ユーザについて複数の異なるグループを割り当て可能とするとき、前記クライアントから受信した前記ログイン要求を検査したあとこれを該ログイン要求一時蓄積部に蓄積し、以降の前記リモート処理要求に対し、その要求に必要な前記所定の権限に応じて、その蓄積された該ログイン要求を切り替えて使用することを特徴とする付記 1 9 に記載のグループ証明書検査部。

#### 【0163】

#### 【発明の効果】

以上説明したように、本発明によれば、従来技術による既述のチケットに比べ高速にチケットすなわちグループ証明書の発行および検査が可能となる。

さらにそのような認証方式において、1つのグループ証明書による複数回のリ

モート処理要求、クライアントサーバ間での相互認証、複数のユーザに対する、同じグループおよび同じ有効期限のグループ証明書の発行、ユーザに割り当てられた複数のグループの取り扱いなどを可能にする。これにより安全性、利便性、効率を高める効果を奏する。

【 0 1 6 4 】

また、複数のユーザの中から、必要に応じて、特定のユーザを調べ出すことのできるログをログファイルに記録することにより、システム 1 0 の安全性と監査能力が一層改善される。

【図面の簡単な説明】

【図 1】

本発明に基づく分散グループ管理システムの基本構成を示す図である。

【図 2】

本発明に基づく分散グループ管理方法の基本ステップを示す図である。

【図 3】

本発明に基づく第 1 実施例を示す図（その 1）である。

【図 4】

本発明に基づく第 1 実施例を示す図（その 2）である。

【図 5】

本発明に基づく第 1 実施例を適用した全体構成例を示す図（その 1）である。

【図 6】

本発明に基づく第 1 実施例を適用した全体構成例を示す図（その 2）である。

【図 7】

パスワード格納手段 2 1 内のデータ構成例を示す図である。

【図 8】

ユーザーグループマッピング格納手段 3 2 内のデータ構成例を示す図である。

【図 9】

グループ秘密情報格納手段 3 3 内のデータ構成例を示す図である。

【図 1 0】

グループ秘密情報格納手段 1 3 内のデータ構成例を示す図である。

【図 1 1】

グループ権限マッピング格納手段 1 5 内のデータ構成例を示す図である。

【図 1 2】

第 1 実施例でのグループ証明書 G C の具体的生成方法を示す図である。

【図 1 3】

第 1 実施例でのグループ証明書 G C の具体的検査方法を示す図である。

【図 1 4】

第 1 実施例のもとでの全体の処理の流れを表す図（その 1）である。

【図 1 5】

第 1 実施例のもとでの全体の処理の流れを表す図（その 2）である。

【図 1 6】

第 1 実施例のもとでのグループ証明書検査部 1 2 の動作の流れを示す図である。

【図 1 7】

本発明に基づく第 2 実施例を示す図（その 1）である。

【図 1 8】

本発明に基づく第 2 実施例を示す図（その 2）である。

【図 1 9】

変形グループ証明書（ログイン要求）G C ' の具体的生成方法を示す図である。

【図 2 0】

第 2 実施例での変形グループ証明書（ログイン要求）G C ' の具体的検査方法を示す図である。

【図 2 1】

変形グループ証明書（ログイン要求）蓄積部 1 4 内に保持されるデータ例を示す図である。

【図 2 2】

第 2 実施例のもとでの全体の処理の流れを表す図（その 1）である。

【図 2 3】

第 2 実施例のもとでの全体の処理の流れを表す図（その 2）である。

【図 2 4】

変形グループ証明書（ログイン要求）検査部 1 2 の動作の流れを示す図（その 1）である。

【図 2 5】

変形グループ証明書（ログイン要求）検査部 1 2 の動作の流れを示す図（その 2）である。

【図 2 6】

本発明に基づく第 3 実施例を示す図（その 1）である。

【図 2 7】

本発明に基づく第 3 実施例を示す図（その 2）である。

【図 2 8】

サーバリプライ r e p の具体的な生成方法を示す図である。

【図 2 9】

サーバリプライ r e p のクライアント側での具体的検査方法を示す図である。

【図 3 0】

第 3 実施例のもとでの全体の処理の流れを表す図（その 1）である。

【図 3 1】

第 3 実施例のもとでの全体の処理の流れを表す図（その 2）である。

【図 3 2】

本発明に基づく第 4 実施例を示す図（その 1）である。

【図 3 3】

本発明に基づく第 4 実施例を示す図（その 2）である。

【図 3 4】

第 4 実施例のもとでの全体の処理の流れを表す図である。

【図 3 5】

本発明に基づく第 5 実施例を示す図（その 1）である。

【図 3 6】

本発明に基づく第 5 実施例を示す図（その 2）である。

【図 3 7】

第 5 実施例のグループ証明書発行装置 3 におけるログファイル 4 8 内のデータ  
の一例を示す図である。

【図 3 8】

第 5 実施例のサーバ 1 におけるログファイル 4 7 内のデータの一例を示す図で  
ある。

【図 3 9】

本発明に基づく第 6 実施例を示す図（その 1）である。

【図 4 0】

本発明に基づく第 6 実施例を示す図（その 2）である。

【図 4 1】

第 6 実施例に基づく証明書識別子 C id の一例を示す図である。

【図 4 2】

本発明に基づく第 7 実施例を示す図（その 1）である。

【図 4 3】

本発明に基づく第 7 実施例を示す図（その 2）である。

【図 4 4】

第 7 実施例に基づくユーザーグループマッピング格納手段 3 2 内のデータの  
一例を示す図である。

【図 4 5】

第 7 実施例で採用するグループ証明書一時蓄積部 5 2 内のデータの一例を示す  
図である。

【図 4 6】

第 7 実施例のもとでの全体の処理の流れを表す図（その 1）である。

【図 4 7】

第 7 実施例のもとでの全体の処理の流れを表す図（その 2）である。

【図 4 8】

従来の分散グループ管理システムを表す図（その 1）である。

【図 4 9】

従来の分散グループ管理システムを表す図（その２）である。

【符号の説明】

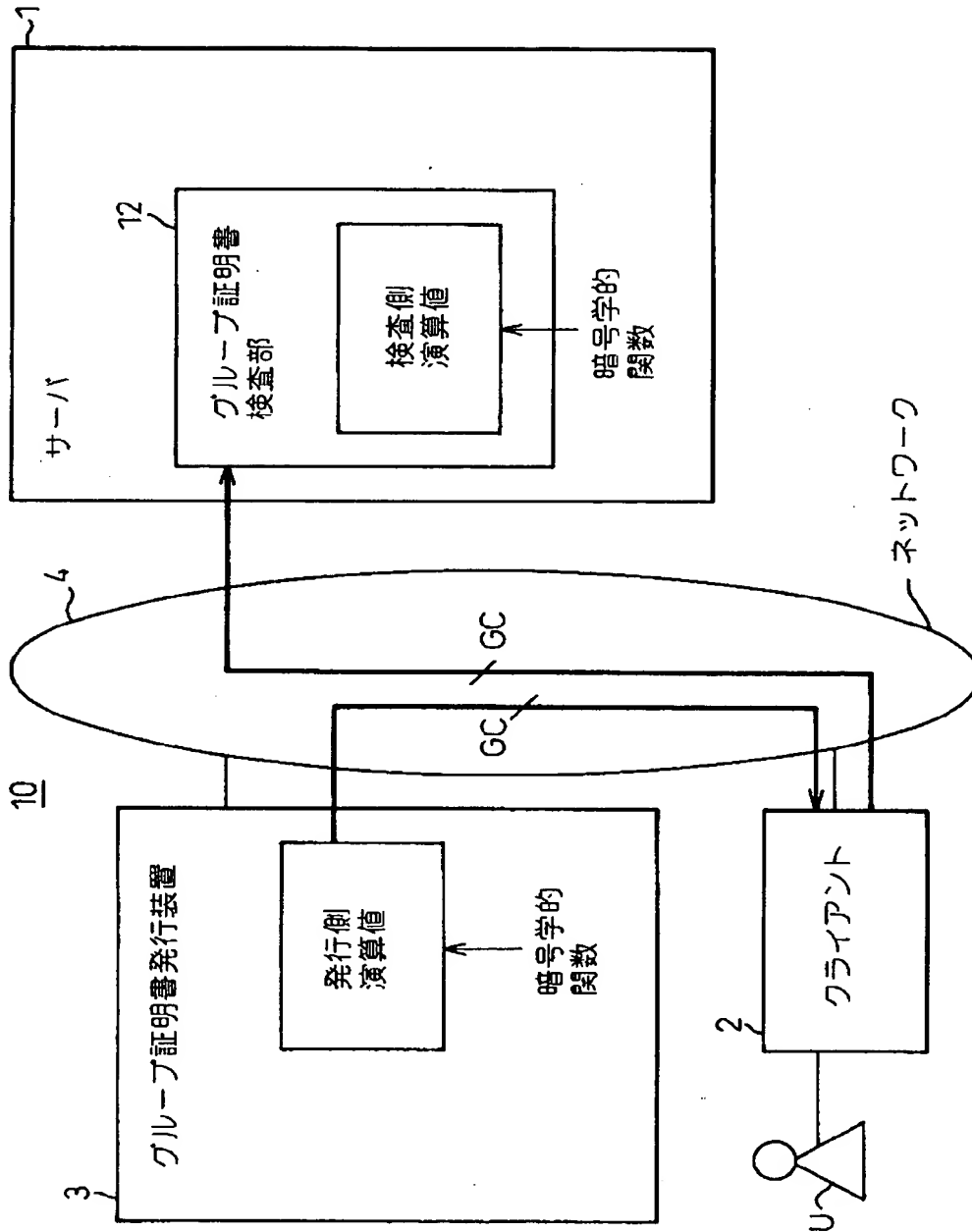
- 1 …サーバ
- 2 …クライアント
- 3 …グループ証明書発行装置
- 3' …チケットサーバ
- 4 …ネットワーク
- 5 …クライアント
- 1 0 …分散グループ管理システム
- 1 1 …認証機能部
- 1 2 …グループ証明書検査部
- 1 3 …グループ秘密情報格納手段
- 1 4 …グループ証明書蓄積部
- 1 5 …グループ権限マッピング格納手段
- 1 6 …ハッシュ機能部（検査側演算部）
- 2 0 …比較手段
- 3 1 …グループ証明書発行部
- 3 2 …ユーザーグループマッピング格納手段
- 3 3 …グループ秘密情報格納手段
- 3 4 …ハッシュ機能部（発行側演算部）
- 4 1 …ハッシュ機能部
- 4 2 …一意識別子生成手段
- 4 3 …比較手段
- 4 5 …暗号処理部
- 4 6 …暗号処理部
- 4 7 …ログファイル
- 4 8 …ログファイル
- 5 1 …一意識別子生成手段
- 5 2 …グループ証明書（ログイン要求）一時蓄積部

【書類名】 図面

【図 1】

図 1

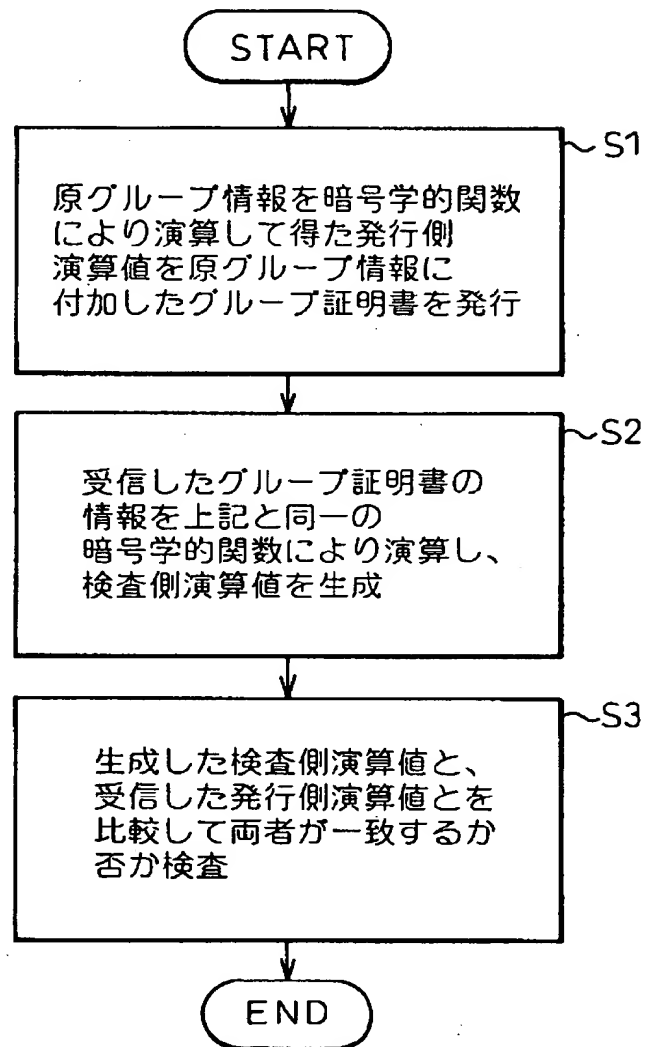
本発明に基づく分散グループ管理システムの基本構成を示す図



【図 2】

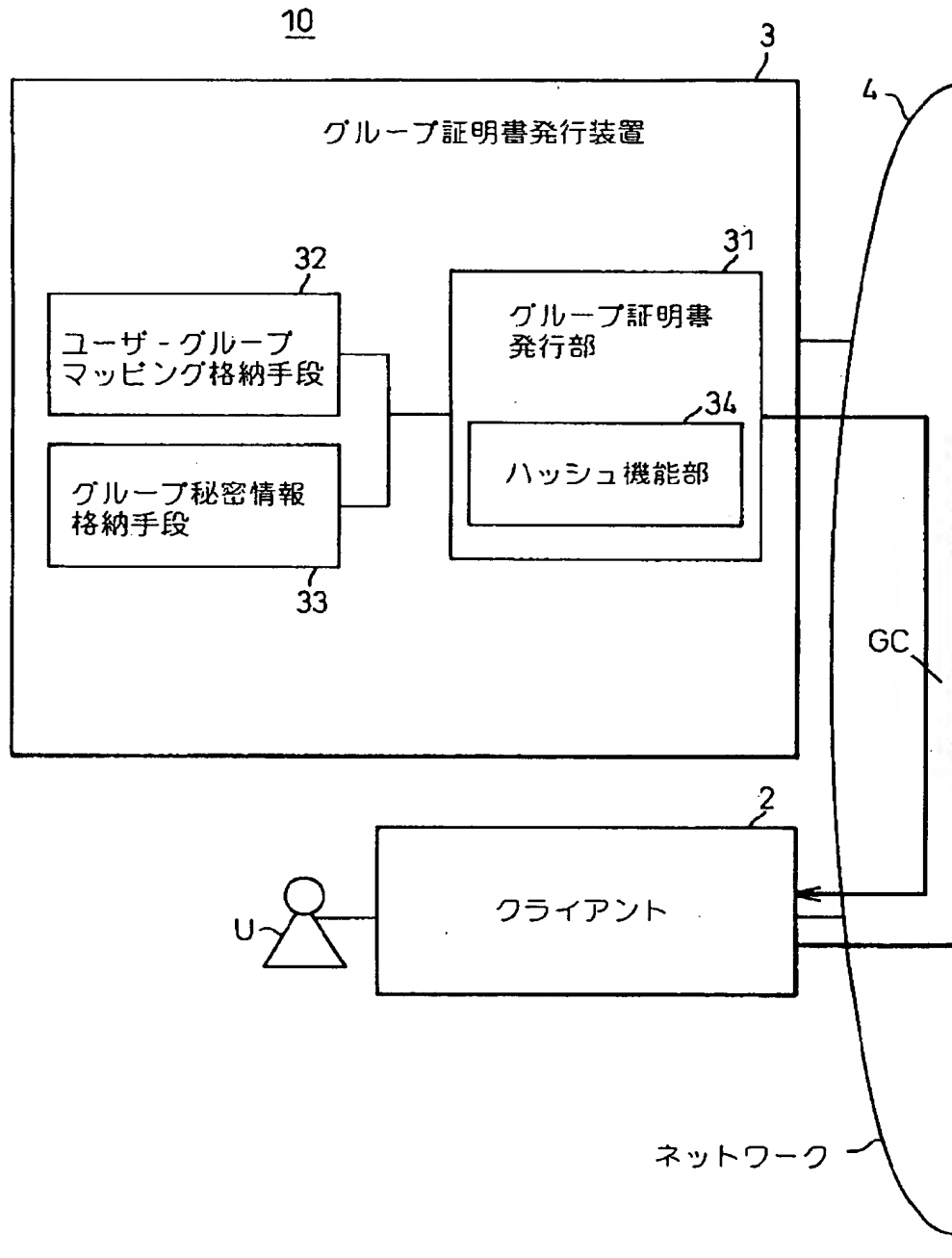
図 2

本発明に基づく分散グループ管理方法の基本ステップを示す図



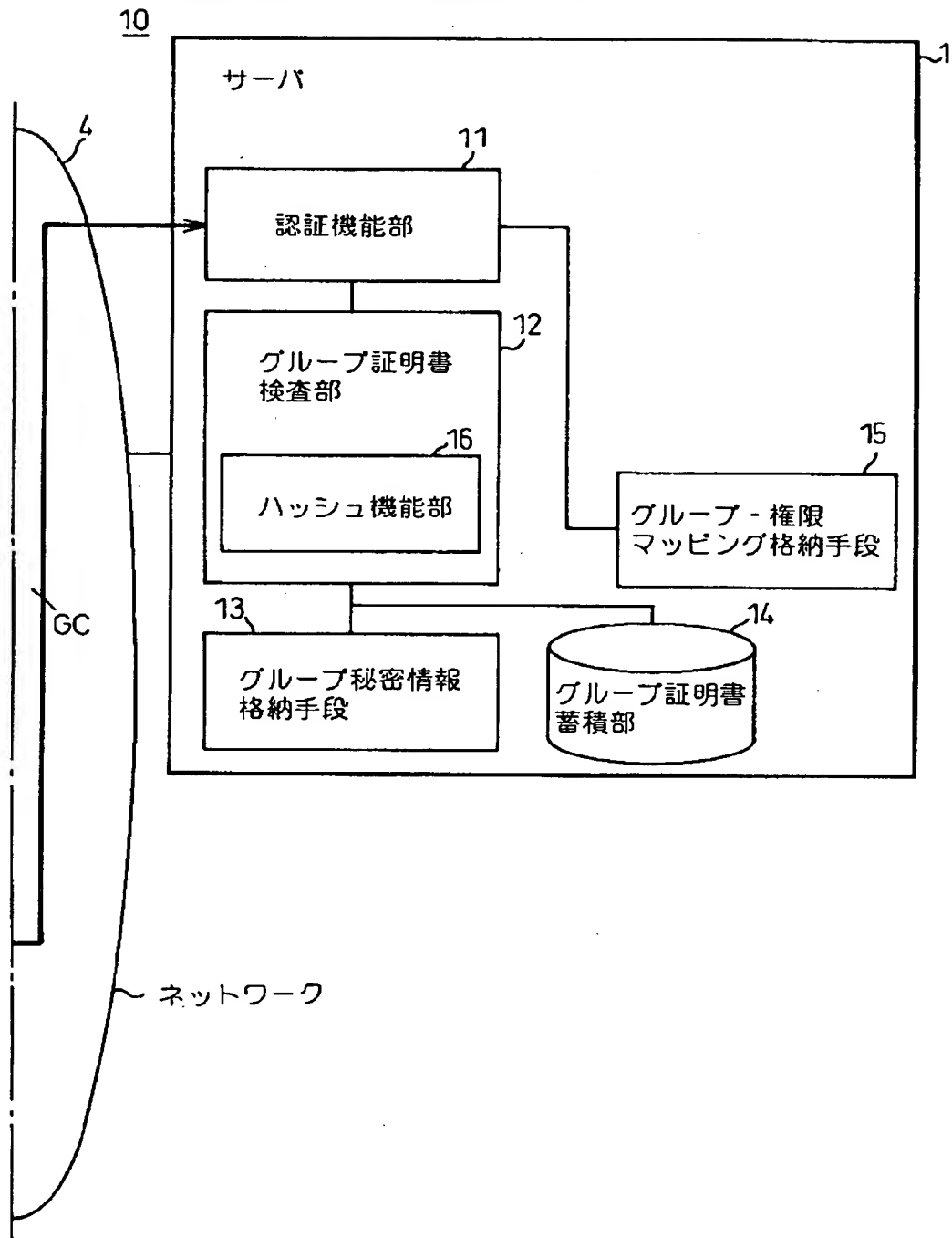
【図3】

図3 本発明に基づく第1実施例を示す図（その1）



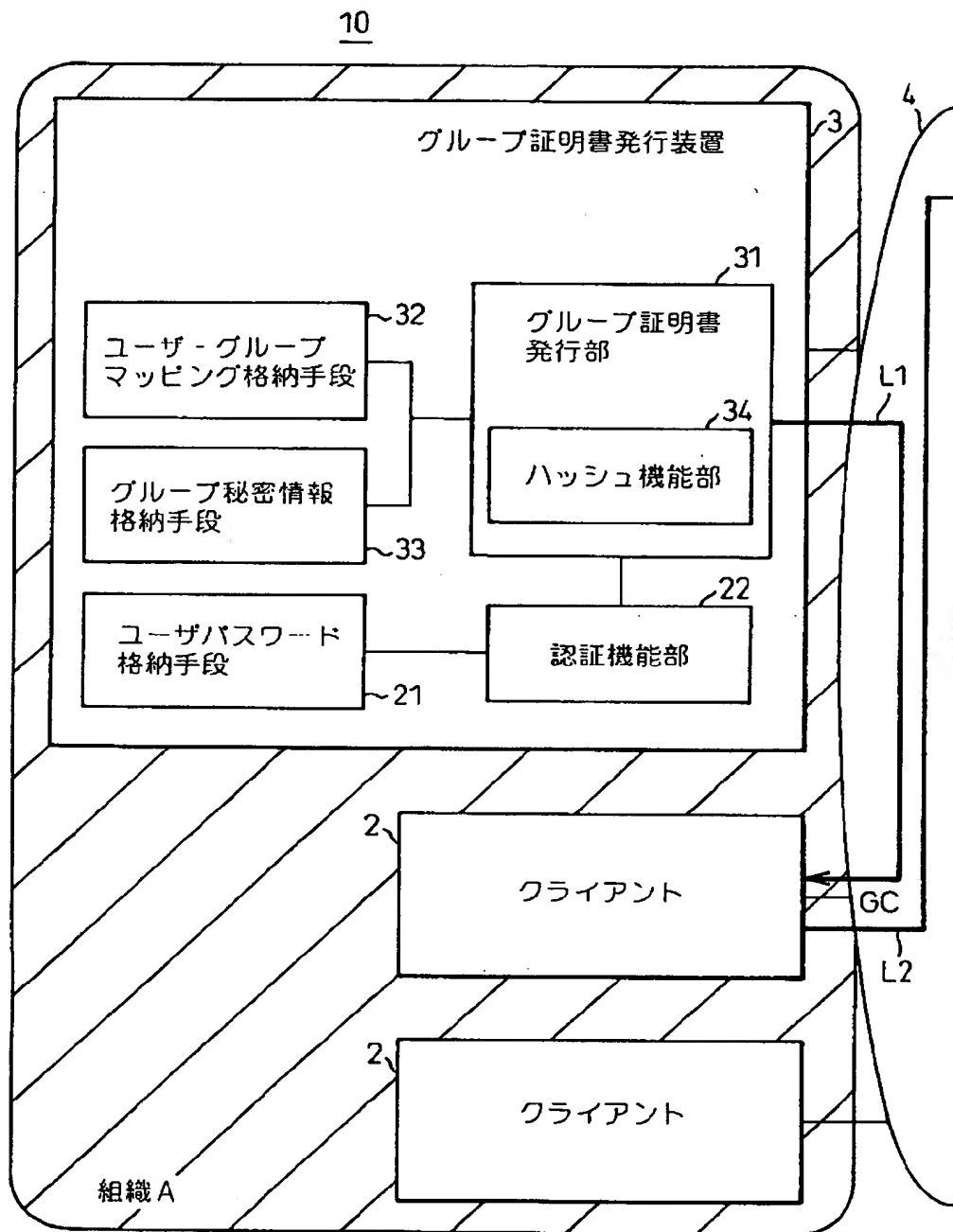
【図 4】

図4 本発明に基づく第1実施例を示す図（その2）



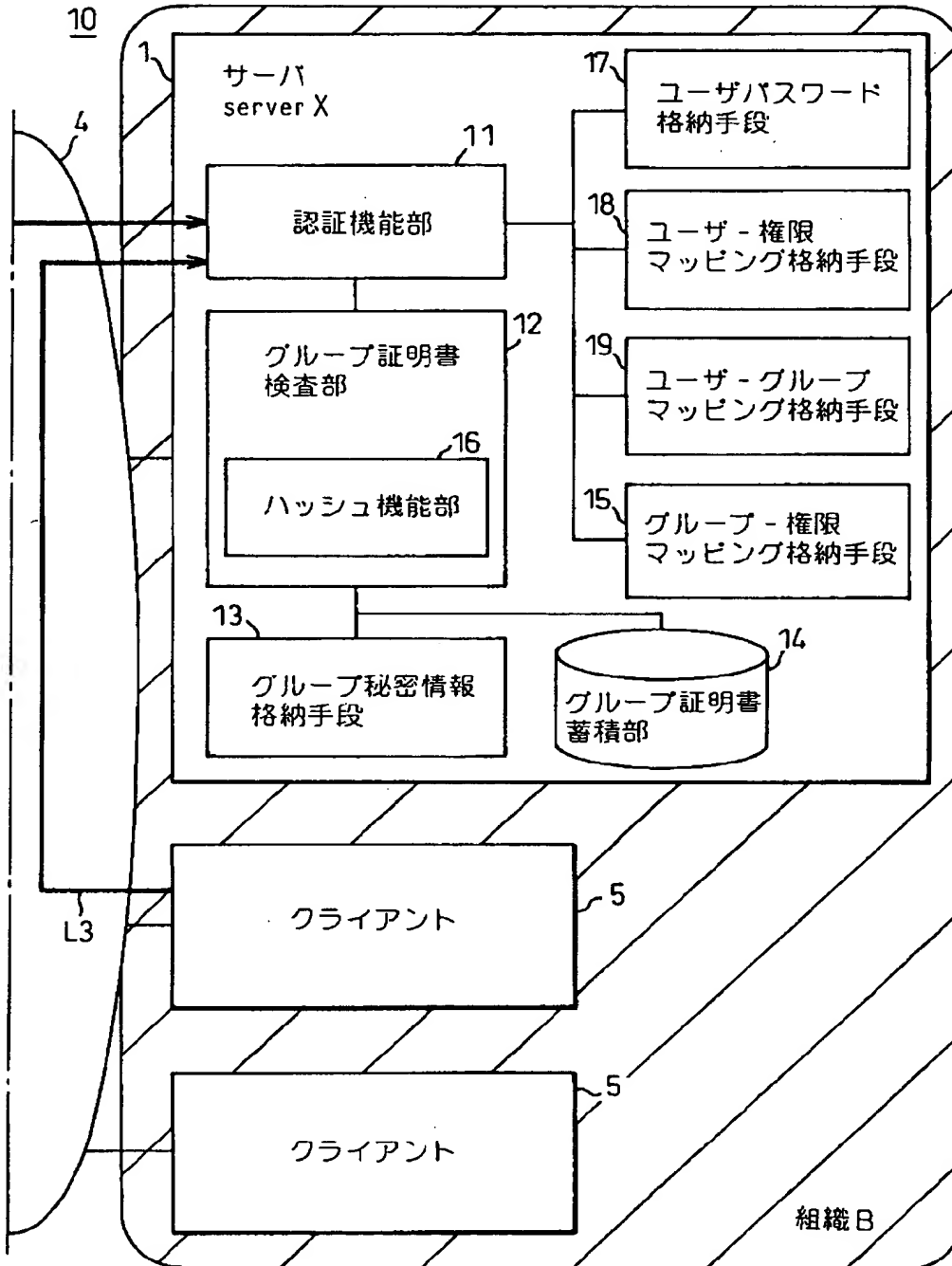
【図 5】

図5 本発明に基づく第1実施例を適用した全体構成例を示す図（その1）



【図 6】

図6 本発明に基づく第1実施例を適用した全体構成例を示す図（その2）



【図 7】

図 7 バスワード格納手段21内のデータ構成例を示す図

21

ユーザ	グループ
server X, user A server X, user B server Y, user A server Y, user C ⋮	server X.group 3 server X.group 1 server Y.group 4 server Y.group 4 ⋮

【図 8】

図 8

ユーザーグループマッピング格納手段32内のデータ構成例を示す図

32


ユーザ	グループ
server X, user A server X, user B server Y, user A server Y, user C ⋮	server X.group 3 server X.group 1 server Y.group 4 server Y.group 4 ⋮

【図 9】

図 9

グループ秘密情報格納手段33内のデータ構成例を示す図

33




グループ	秘密情報
server X.group 1 server X.group 2 server X.group 3 server Y.group 4 ⋮	secret 1 secret 2 secret 3 secret 4 ⋮

【図 1 0】

図 10

グループ秘密情報格納手段13内のデータ構成例を示す図

13



グループ	秘密情報
group 1 group 2 group 3 ⋮	secret 1 secret 2 secret 3 ⋮

【図 1 1】

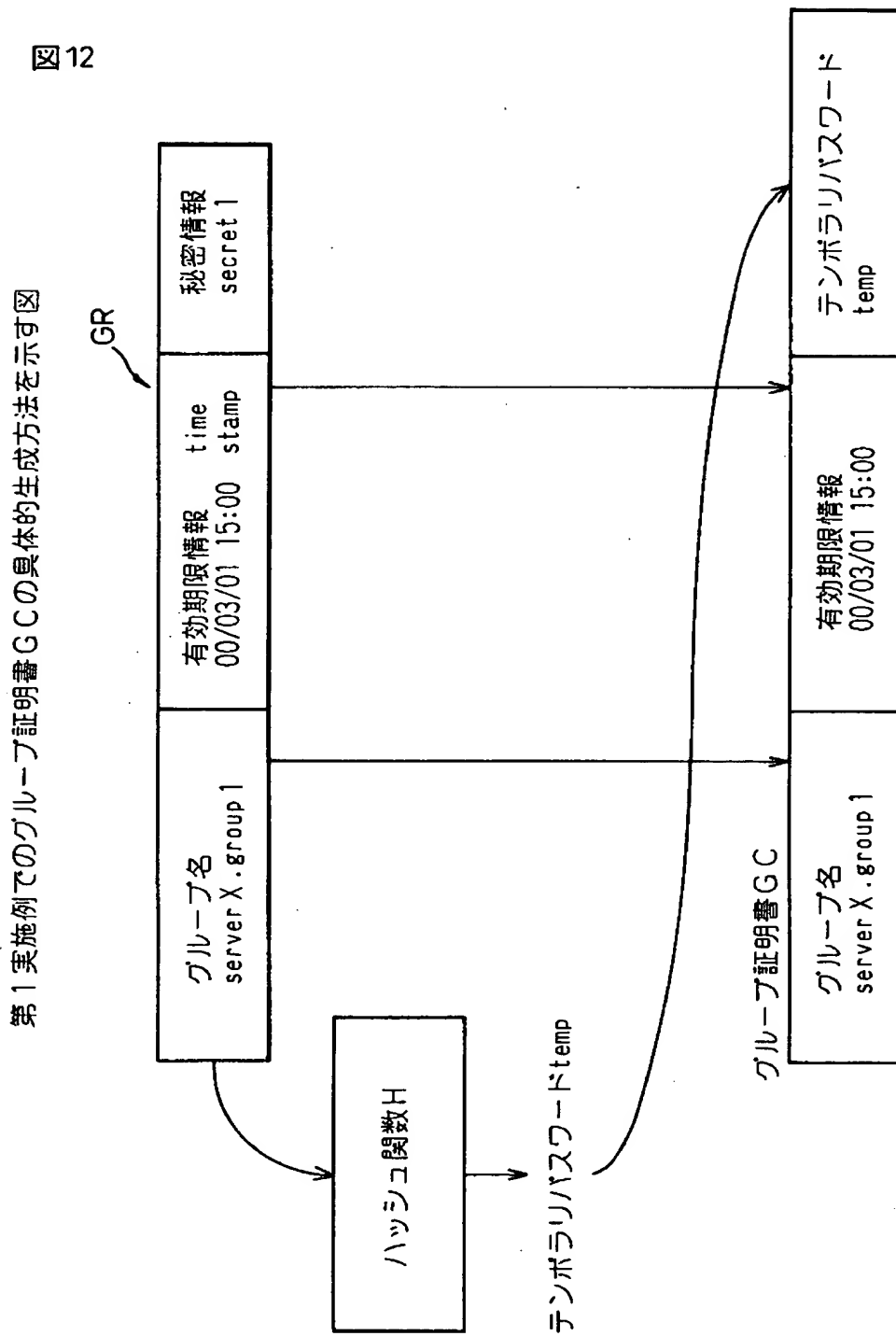
図 11

グループ権限マッピング格納手段15内のデータ構成例を示す図

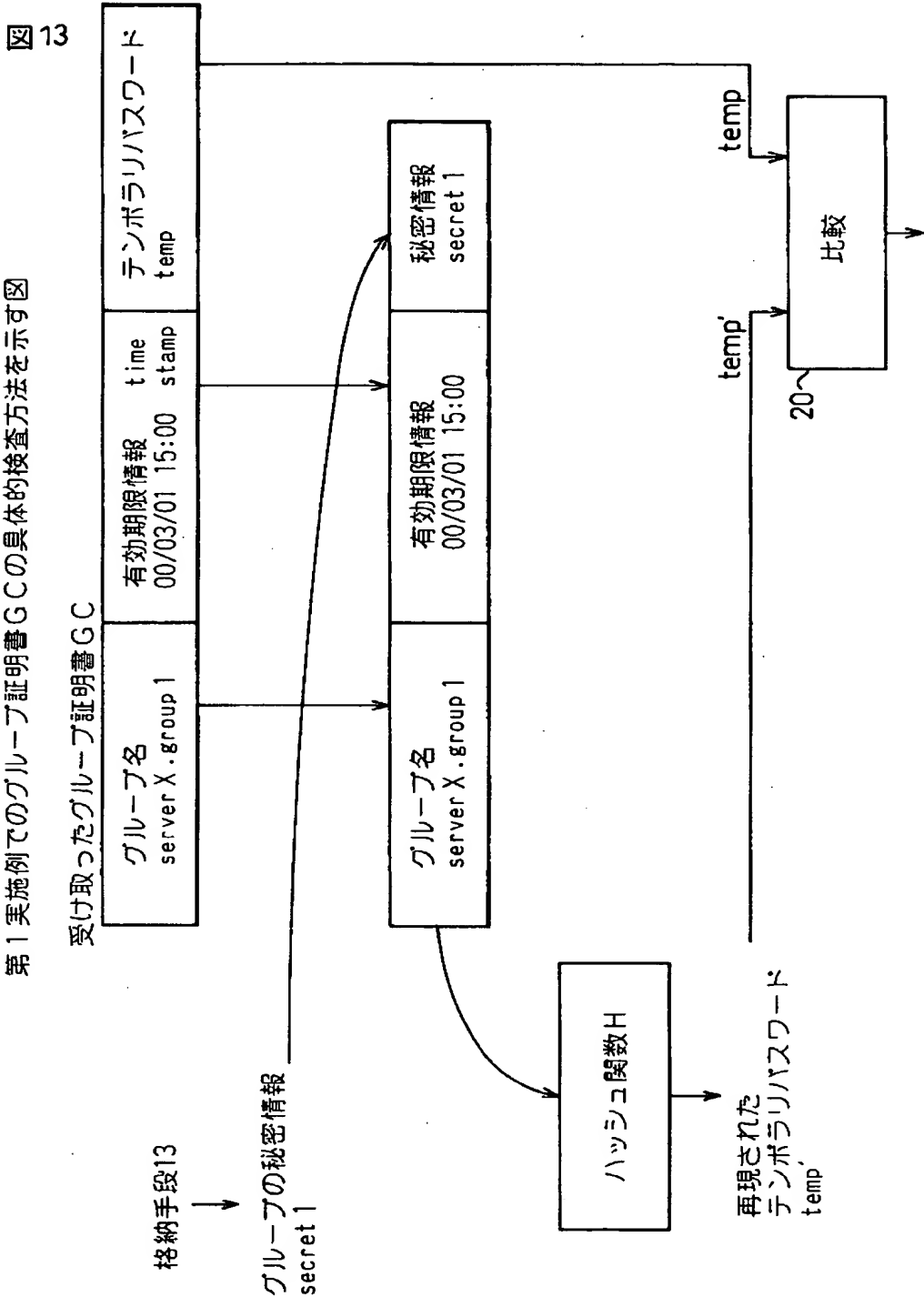
15

グループ名	権限	
	対象	内容
group 1	fileA	r-
group 1	fileB	—
group 2	fileA	rw
group 2	fileB	r-
group 3	fileA	rw
group 3	fileB	rw
⋮	⋮	⋮

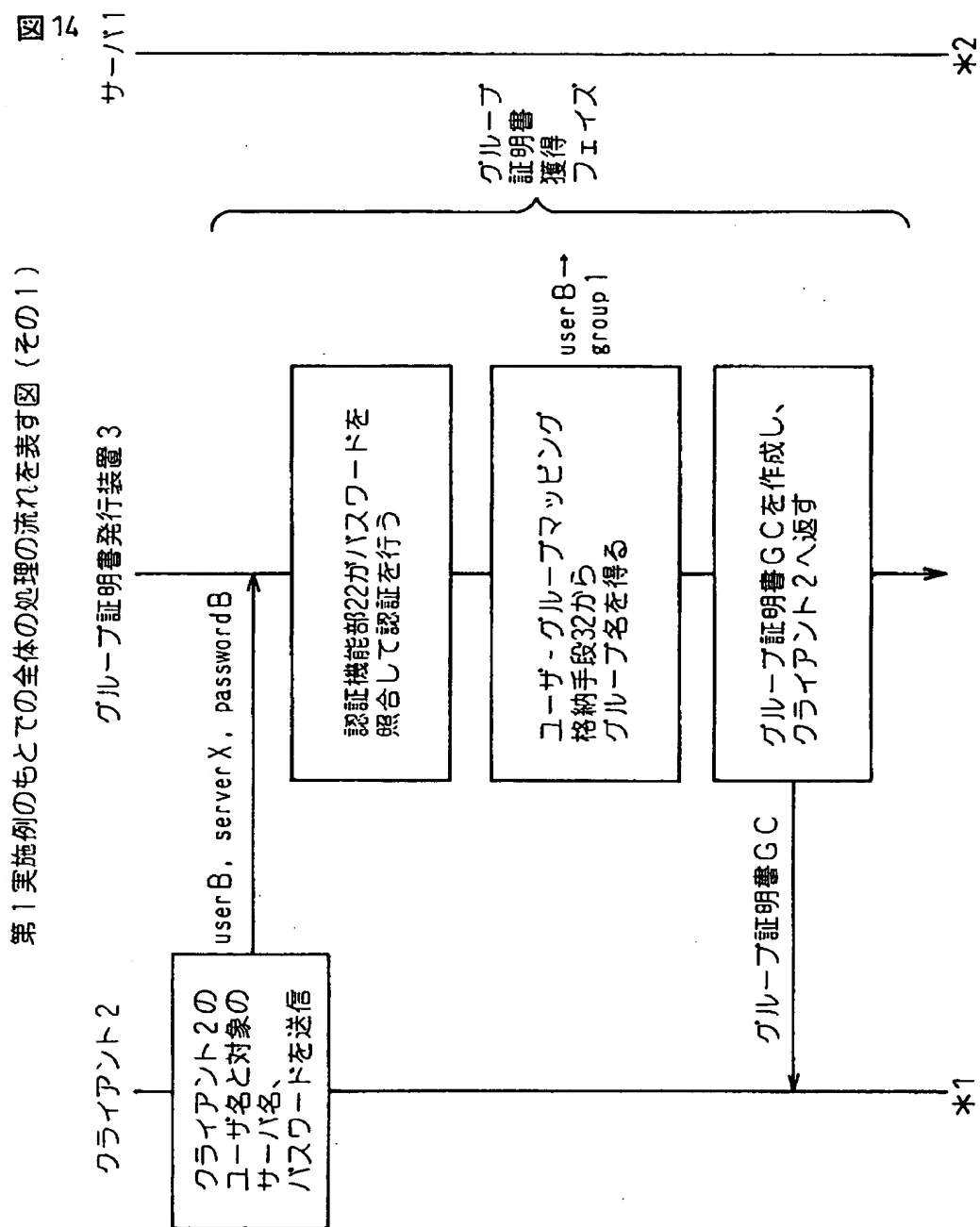
【図 1 2】



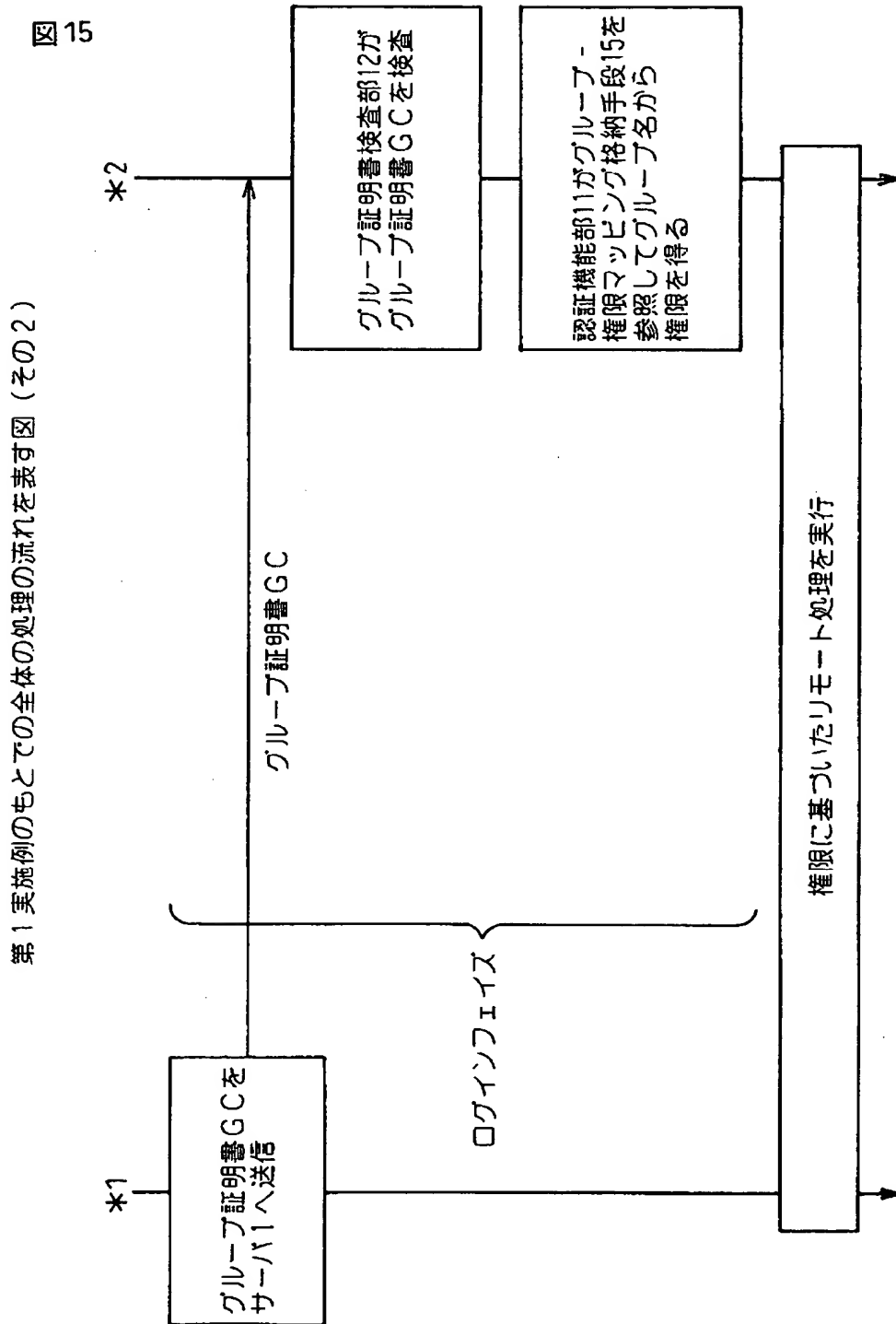
【図 1 3】



【図 1 4】



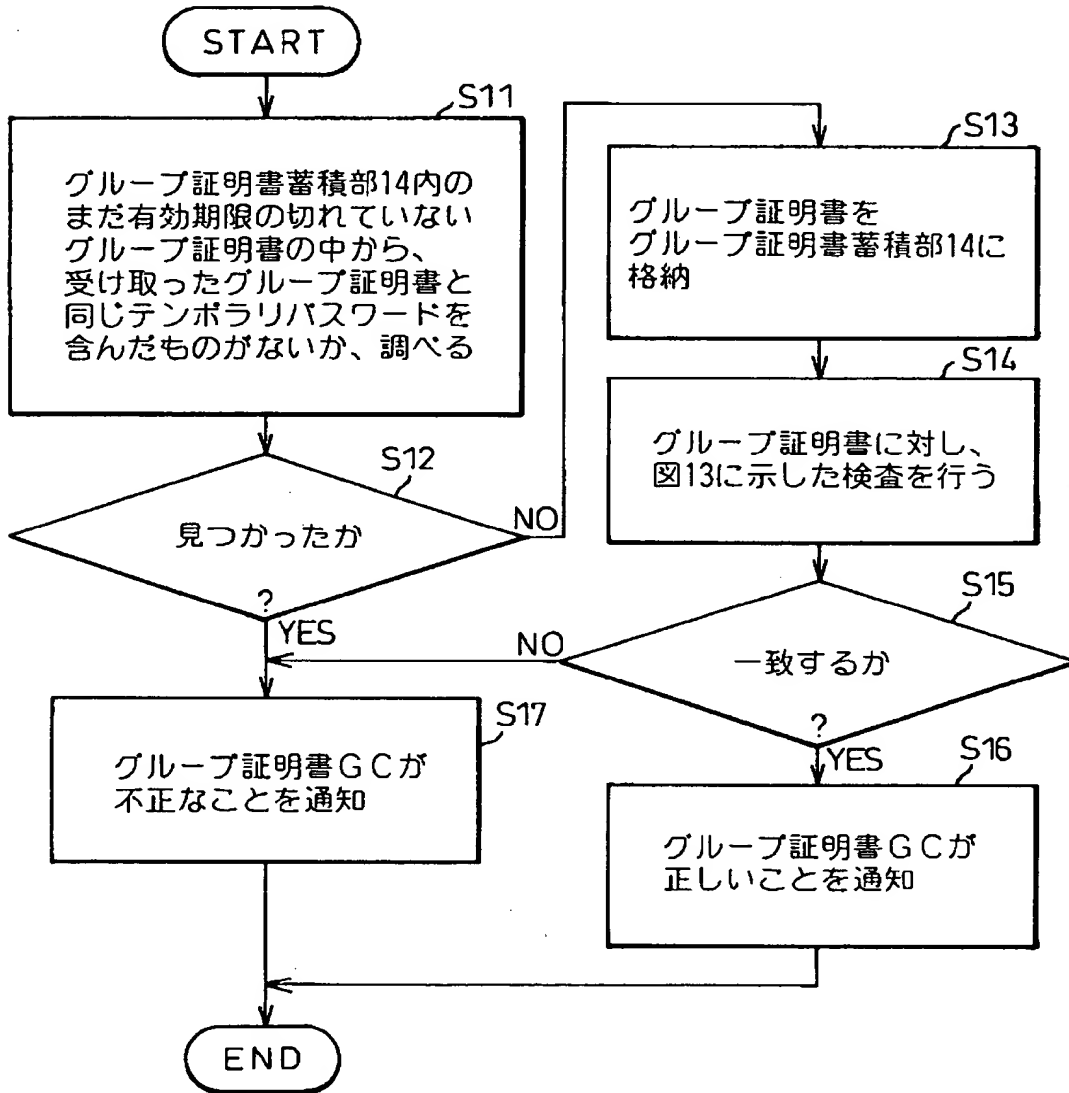
【図 1 5】



【図 1 6】

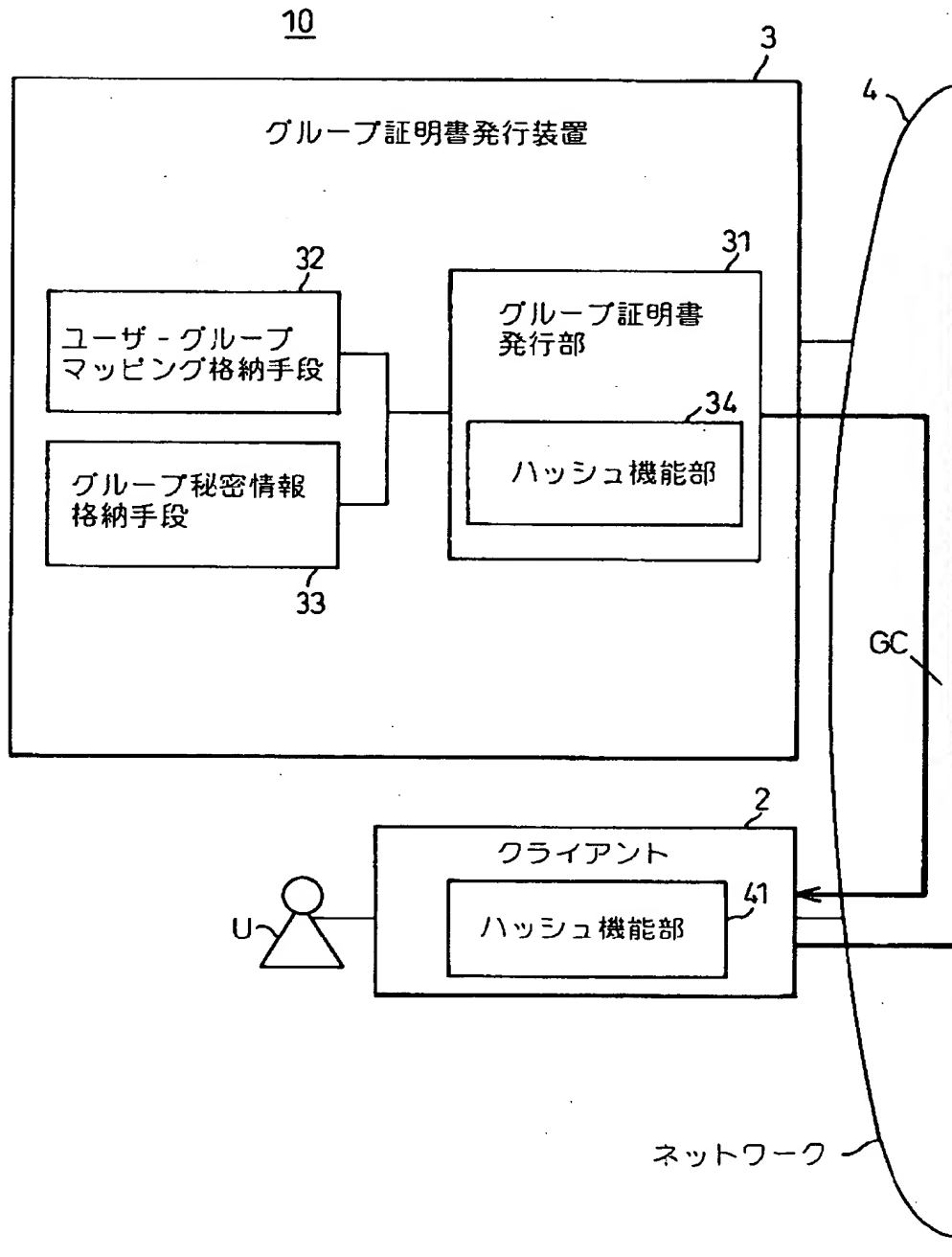
図 16

第 1 実施例のもとでのグループ証明書検査部 12 の動作の流れを示す図

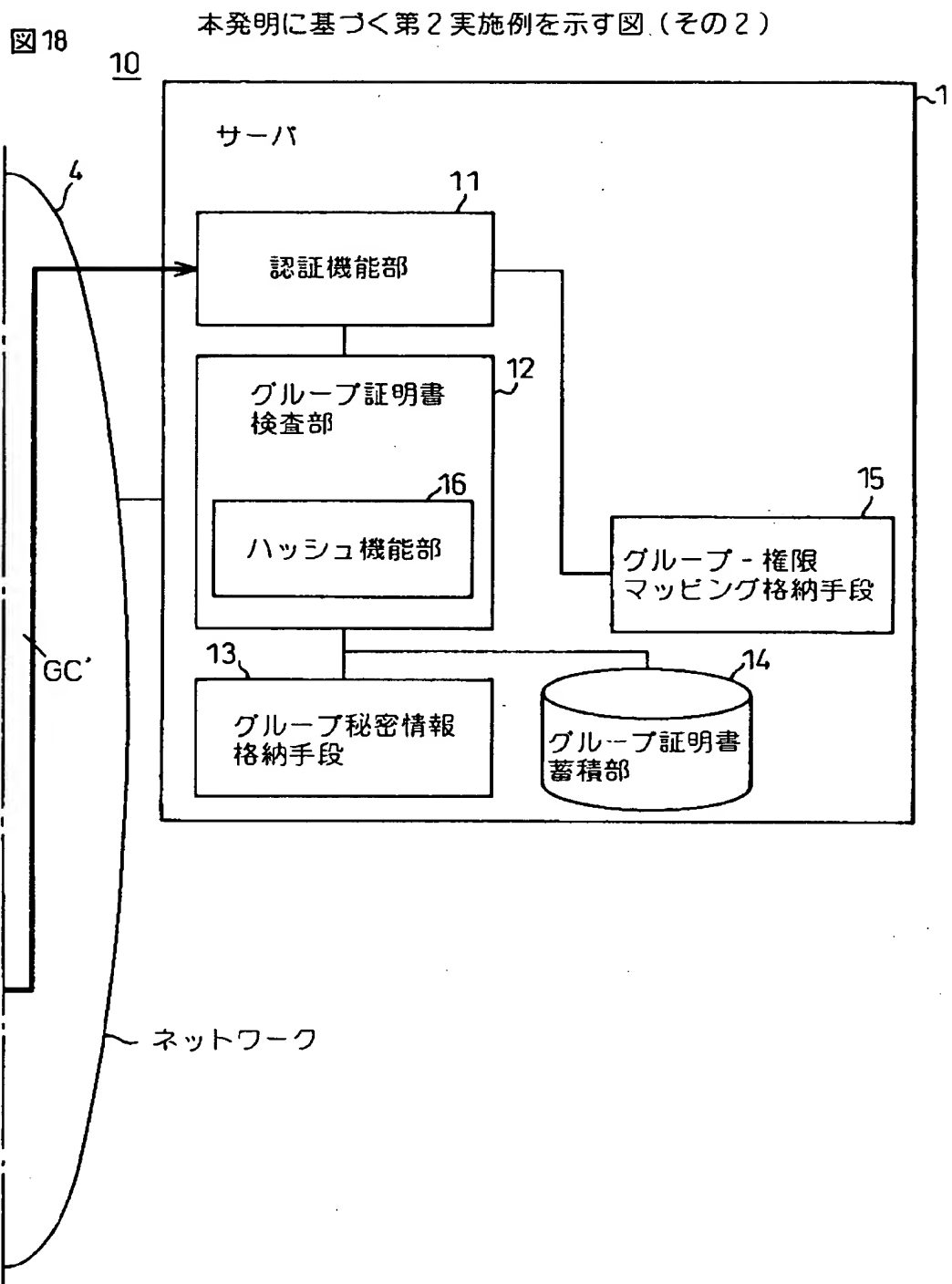


【図 17】

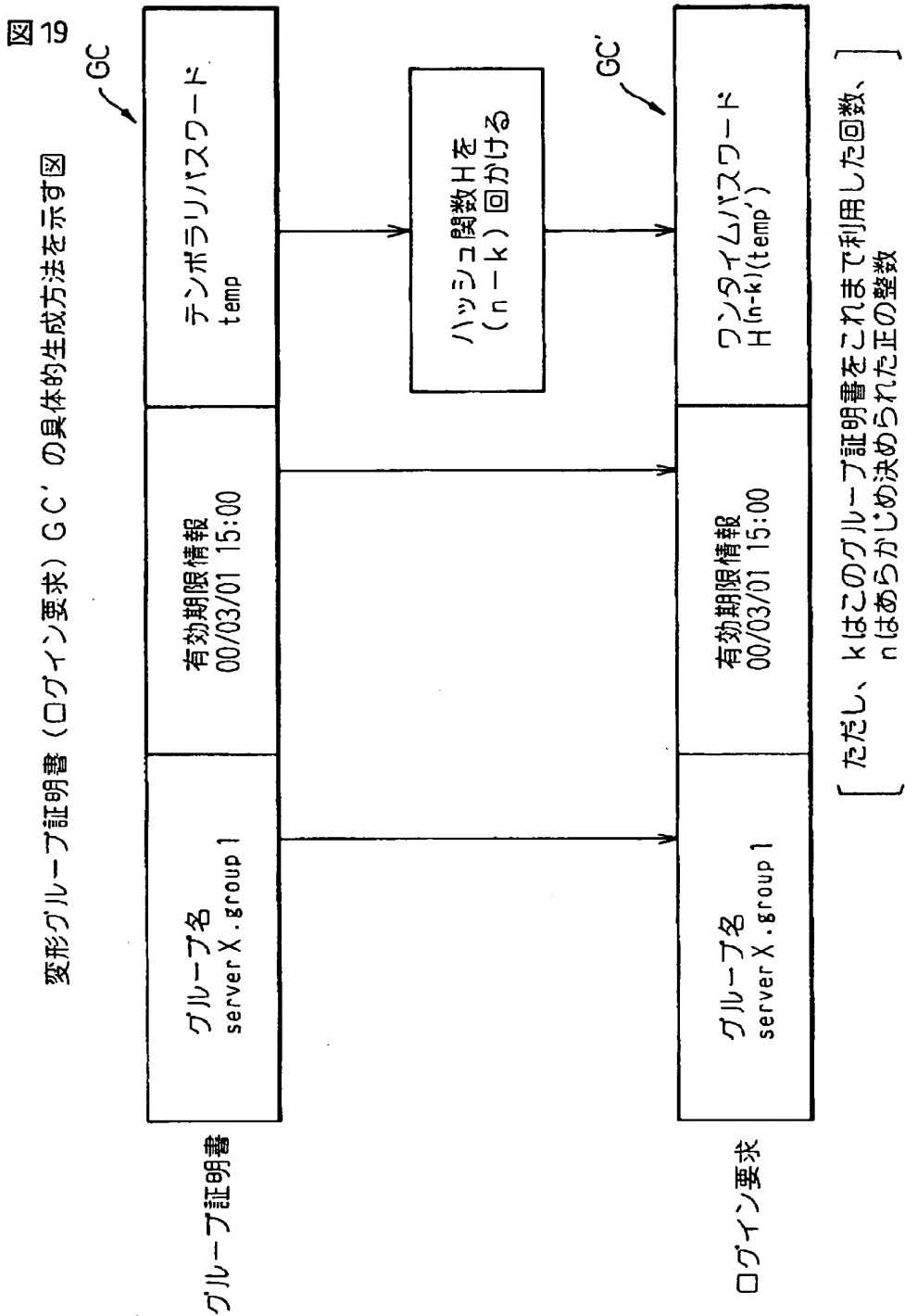
図 17 本発明に基づく第 2 実施例を示す図（その 1）



【図 18】

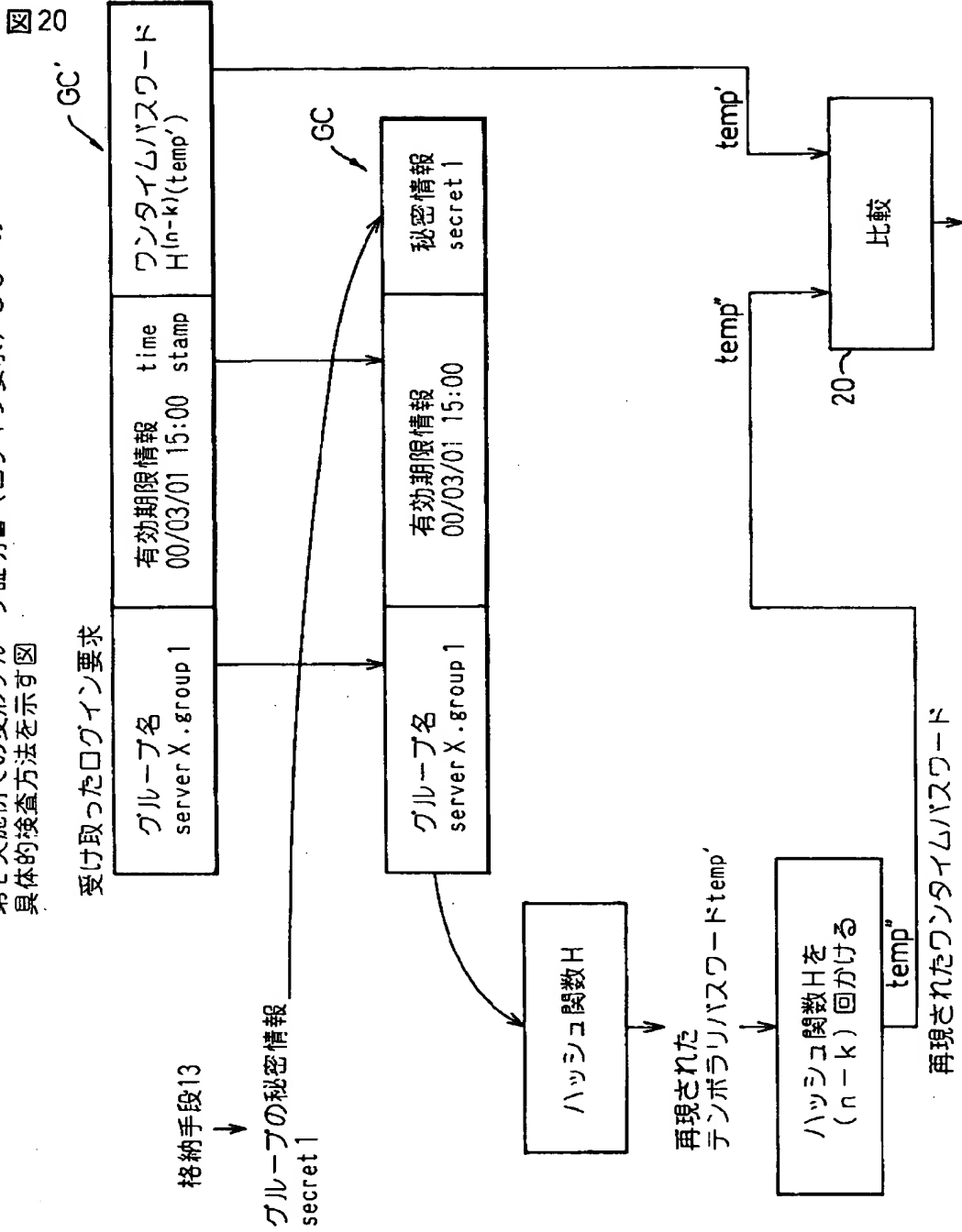


【図 1 9】



【図 20】

第2実施例での変形グループ証明書（ログイン要求）GC' の  
具体的検査方法を示す図



【図 2 1】

変形グループ証明書（ログイン要求）蓄積部14内に保持されるデータ例を示す図

図21

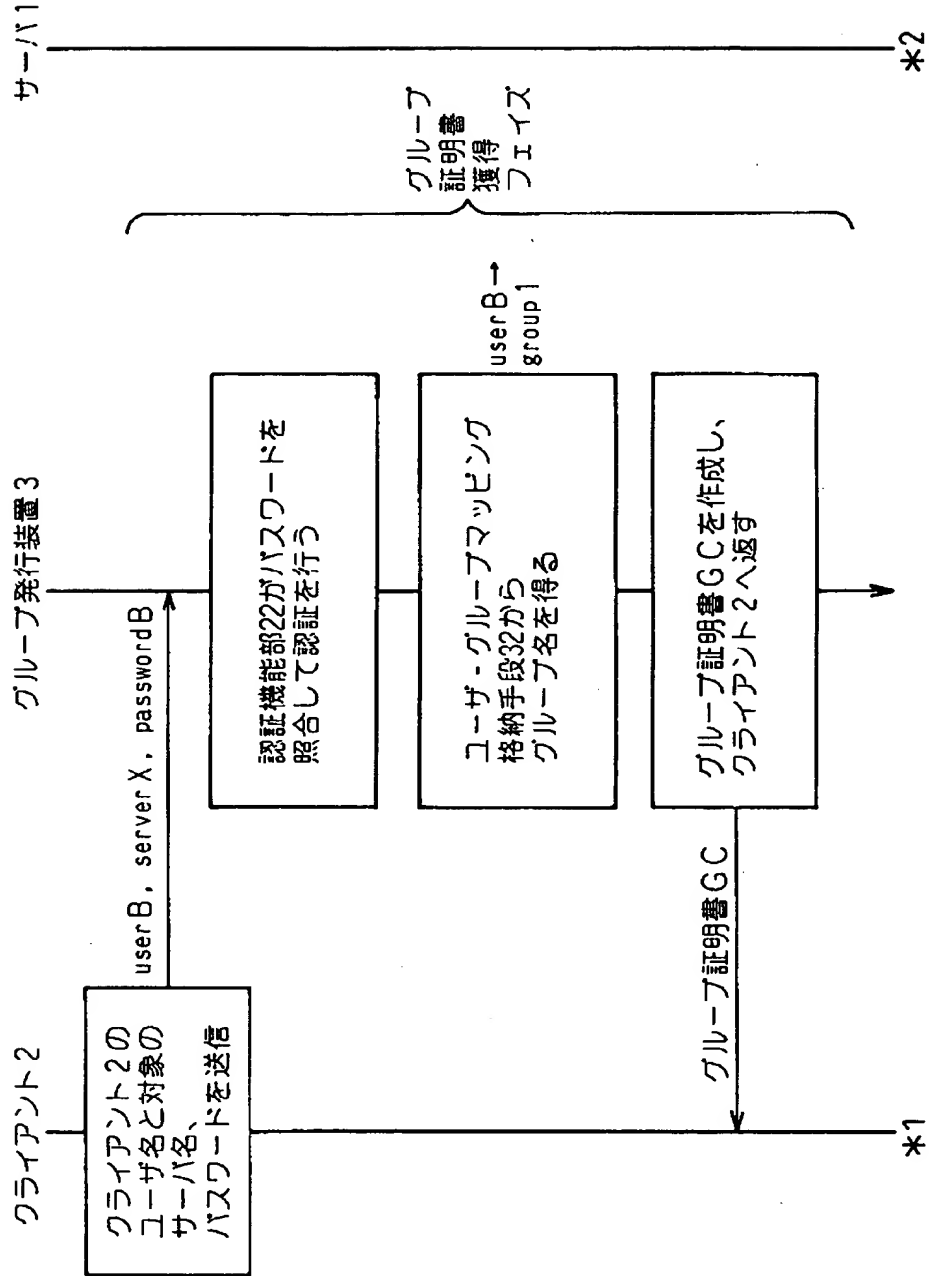
14

ログイン要求GC'			kの値
グループ名	有効期限情報 time stamp	ワンタイムパスワード temp'	
server X.group 1 server X.group 4 server X.group 2 ⋮	00/03/01 15:00 00/03/01 13:00 00/03/01 14:00 ⋮	H <sup>(n)</sup> (temp') H <sup>(n-4)</sup> (temp') H <sup>(n-6)</sup> (temp') ⋮	0 4 6 ⋮

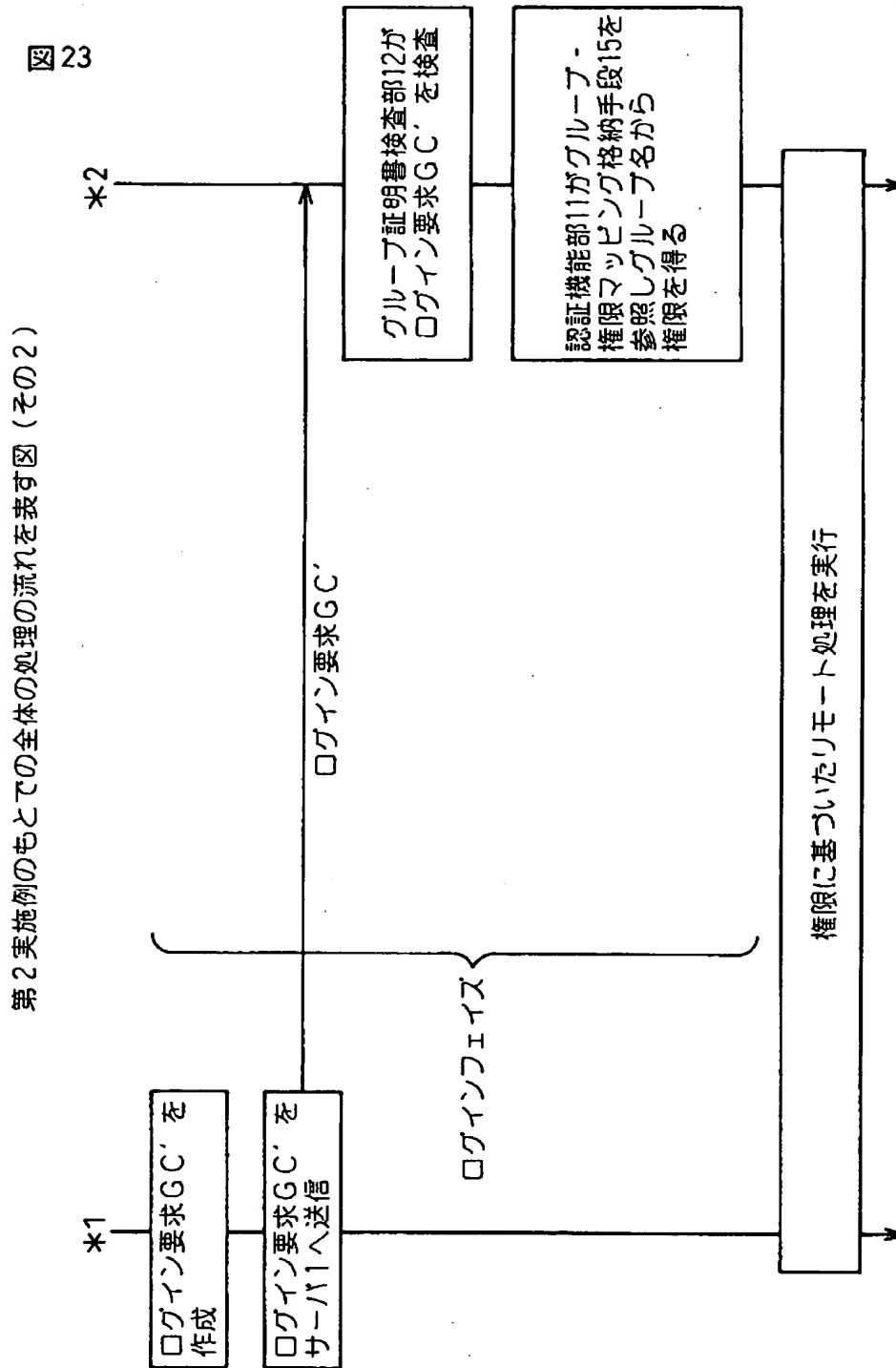
【図 2 2】

図 22

第 2 実施例のもとでの全体の処理の流れを表す図（その 1）



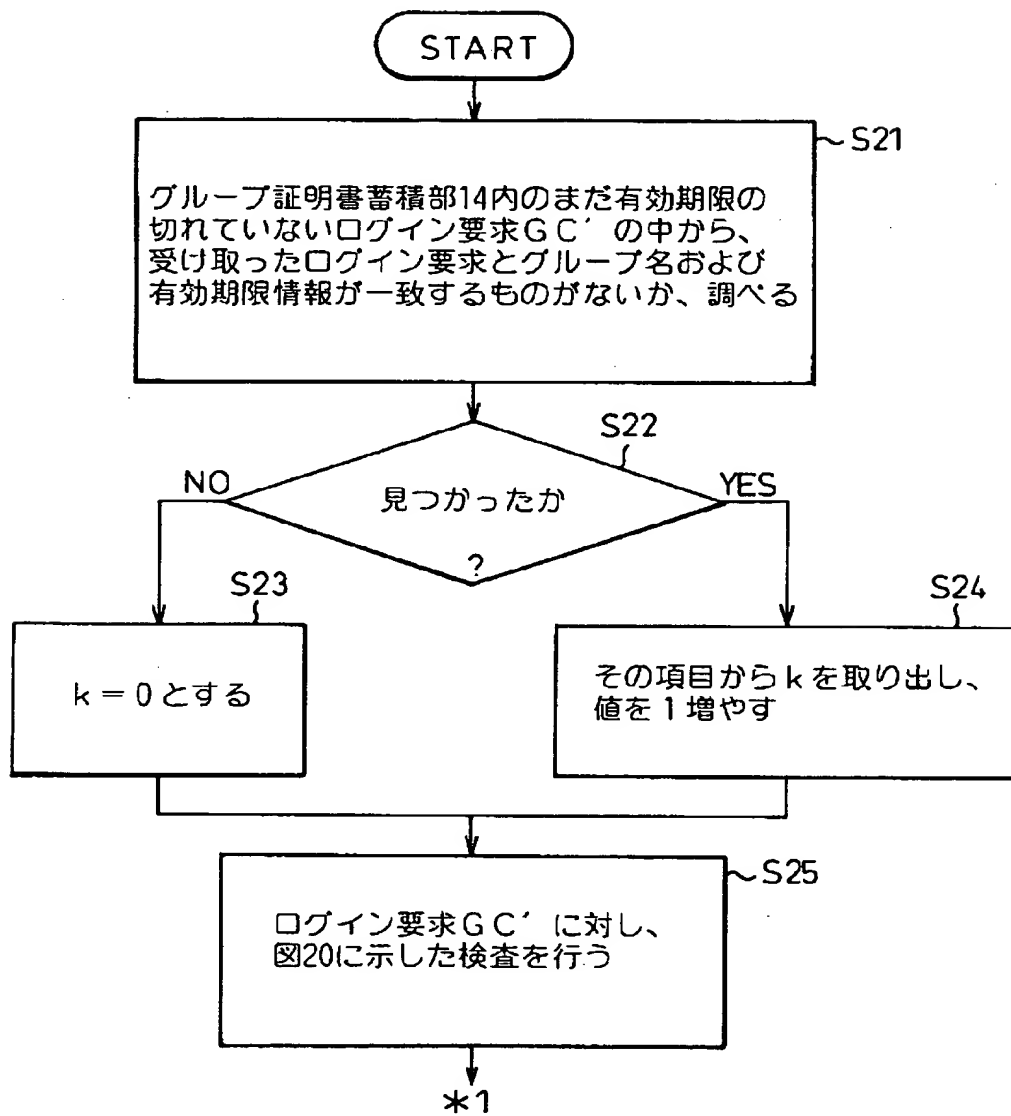
【図 2 3】



【図 2 4】

図 24

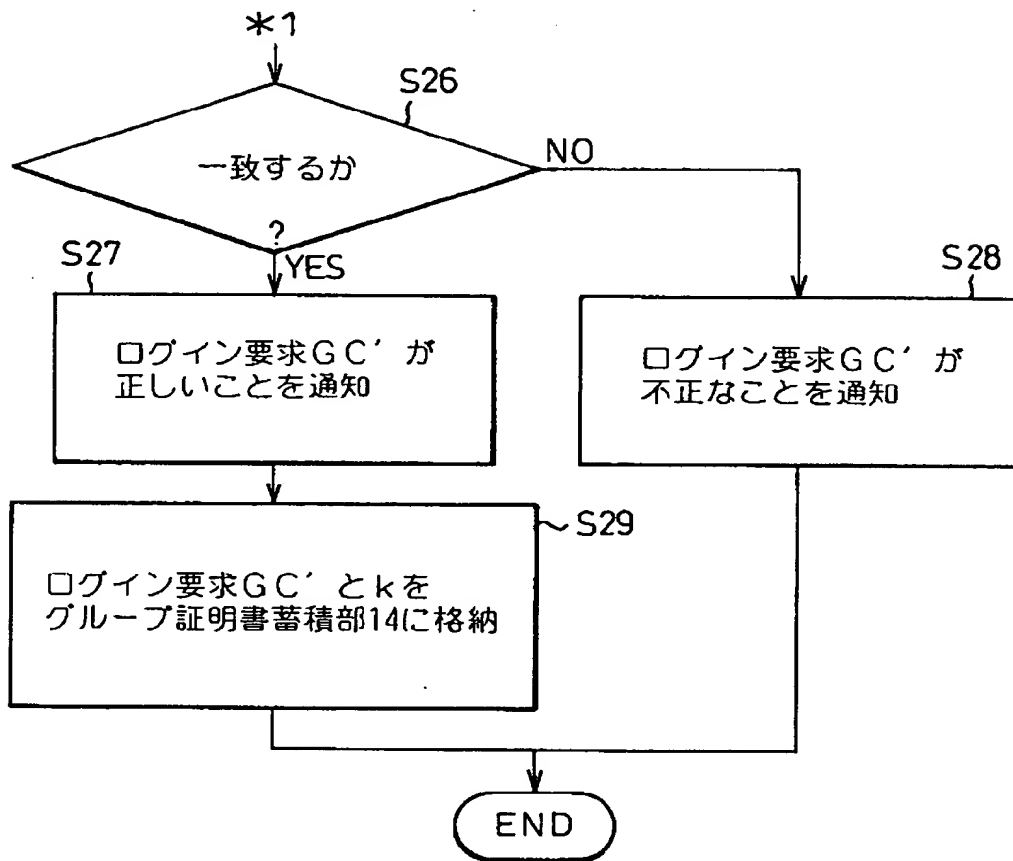
変形グループ証明書（ログイン要求）検査部12の  
動作の流れを示す図（その1）



【図 2 5】

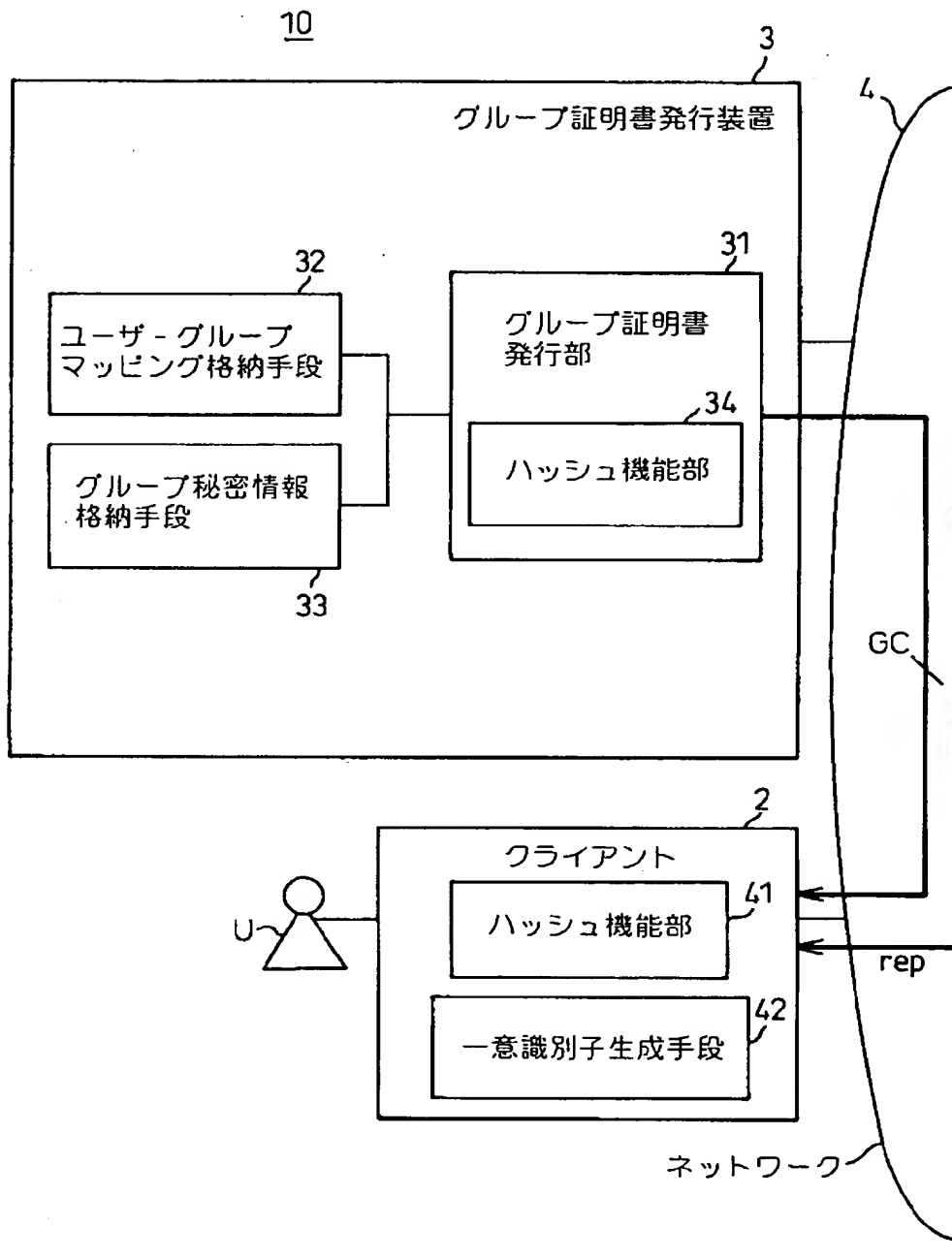
図25

変形グループ証明書（ログイン要求）検査部12の  
動作の流れを示す図（その2）



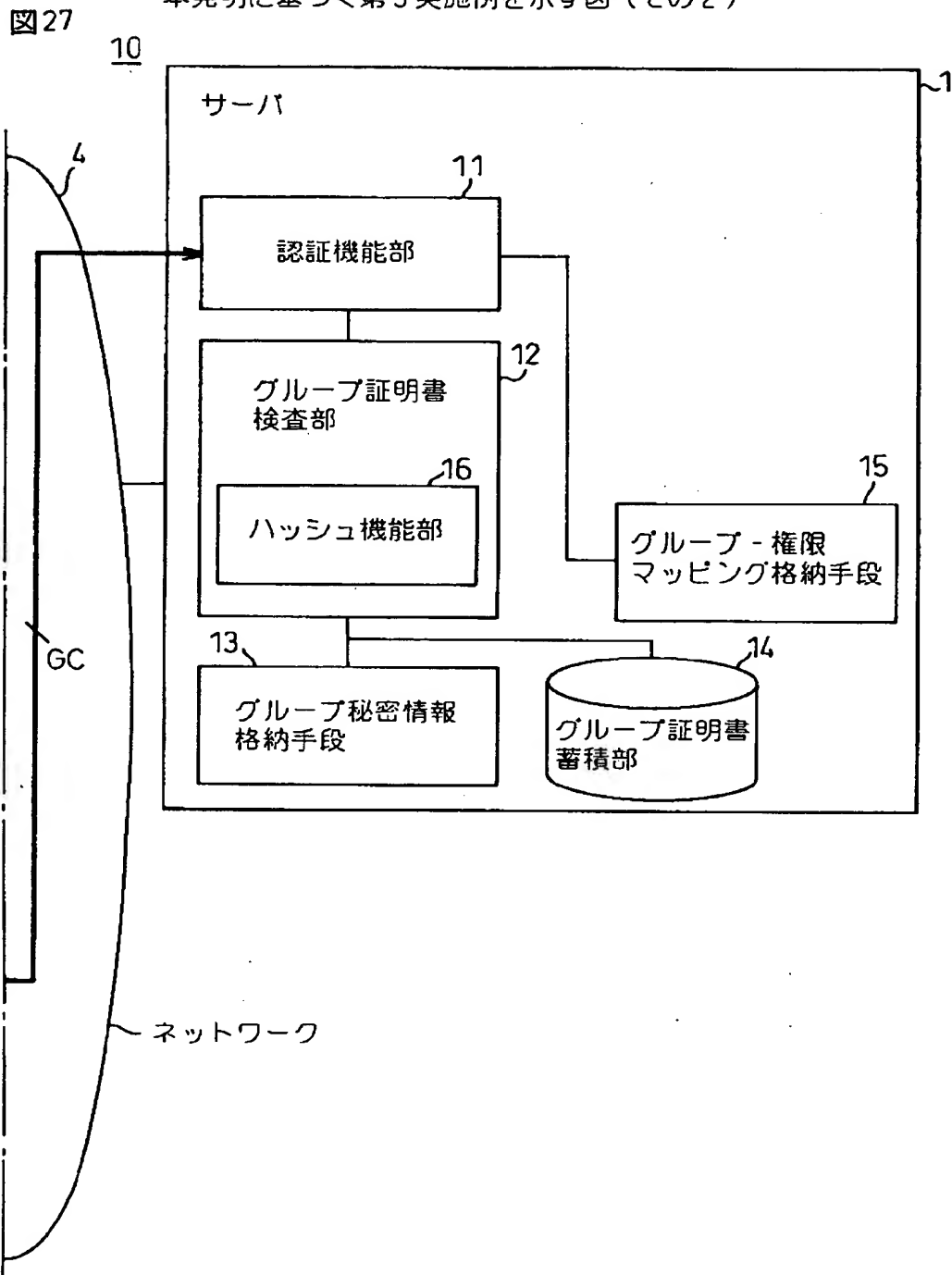
【図 26】

図26 本発明に基づく第3実施例を示す図（その1）

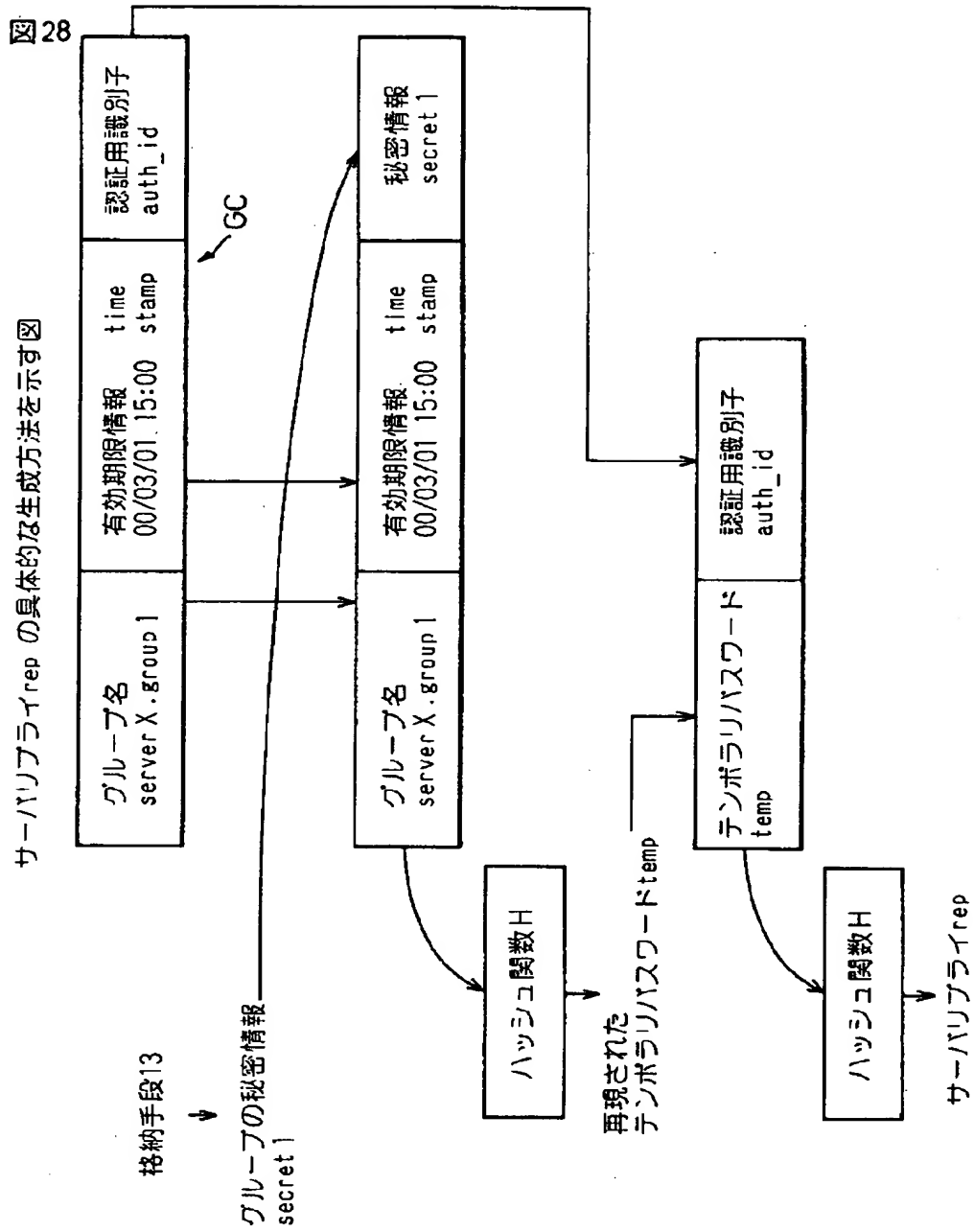


【図 27】

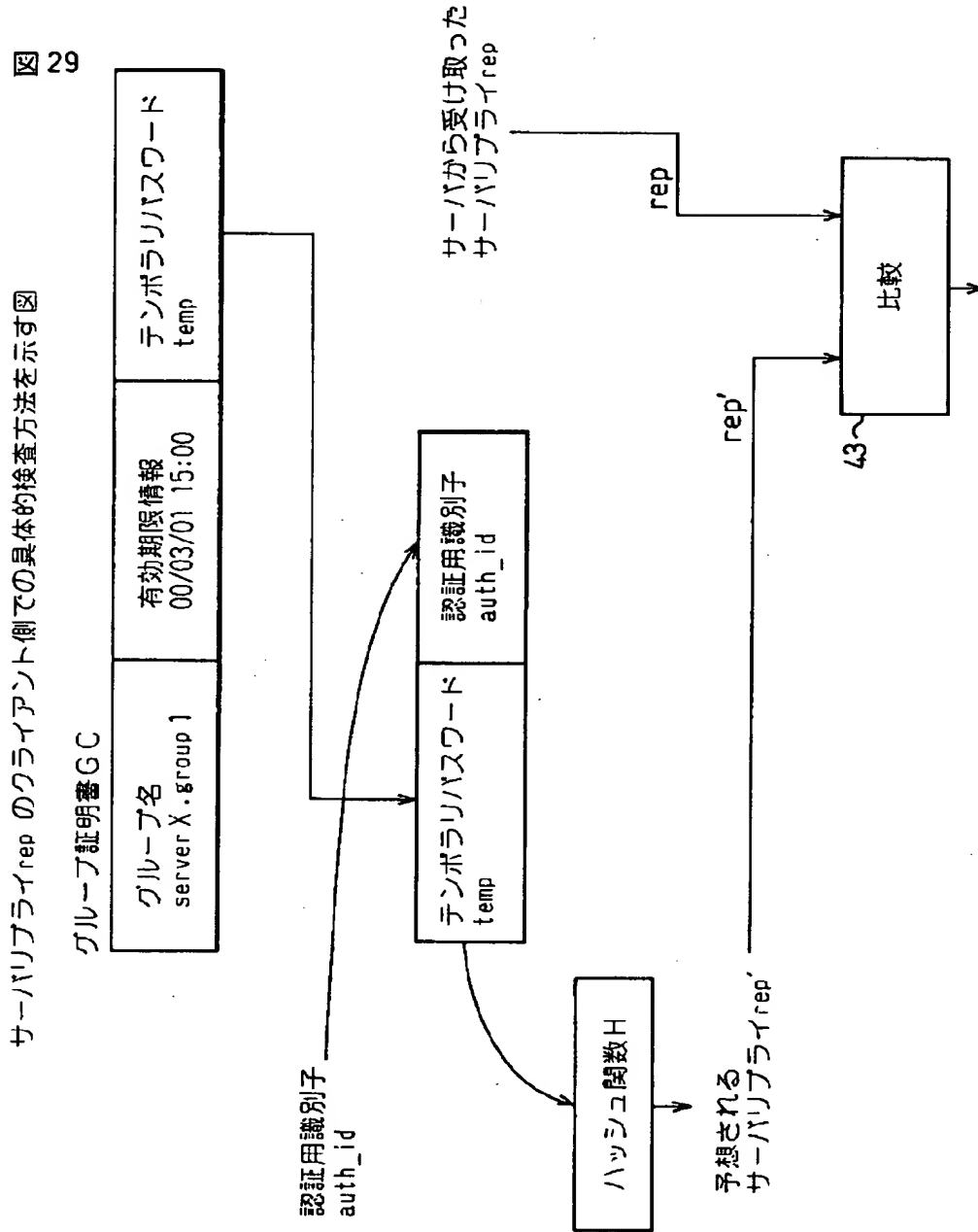
本発明に基づく第3実施例を示す図（その2）



【図 2 8】



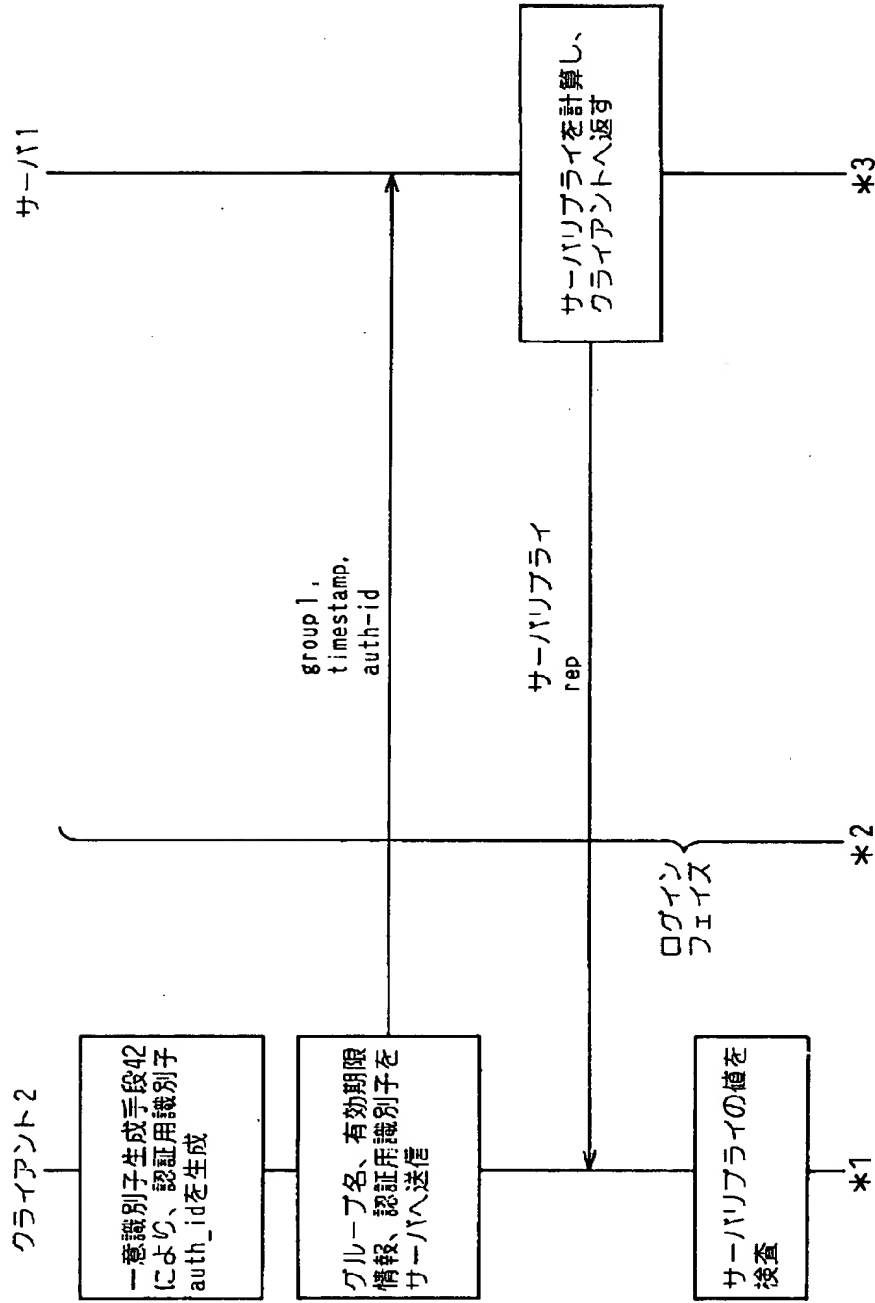
【図 2 9】



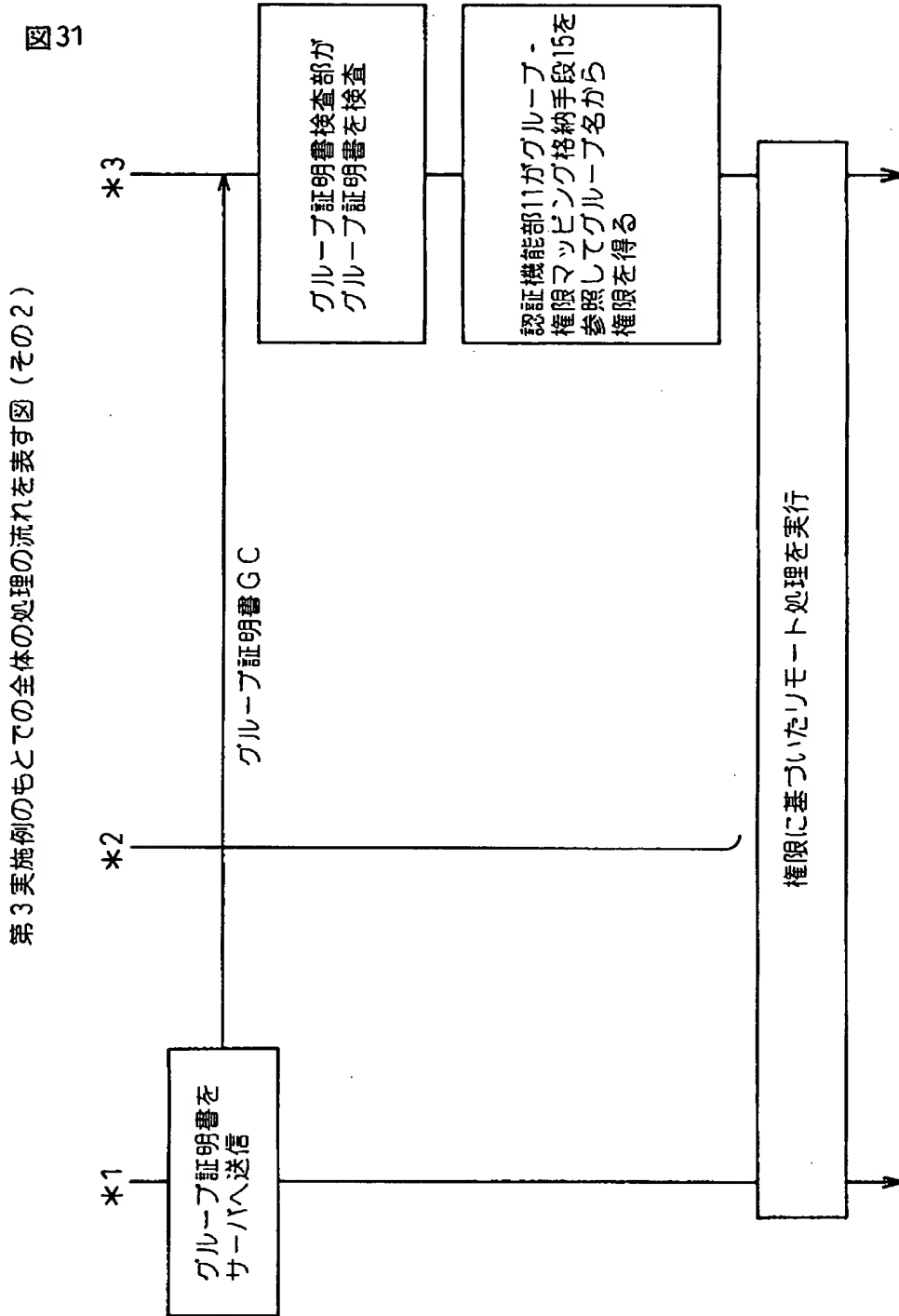
【図 3 0】

図 30

第 3 実施例のもとでの全体の処理の流れを表す図（その 1）

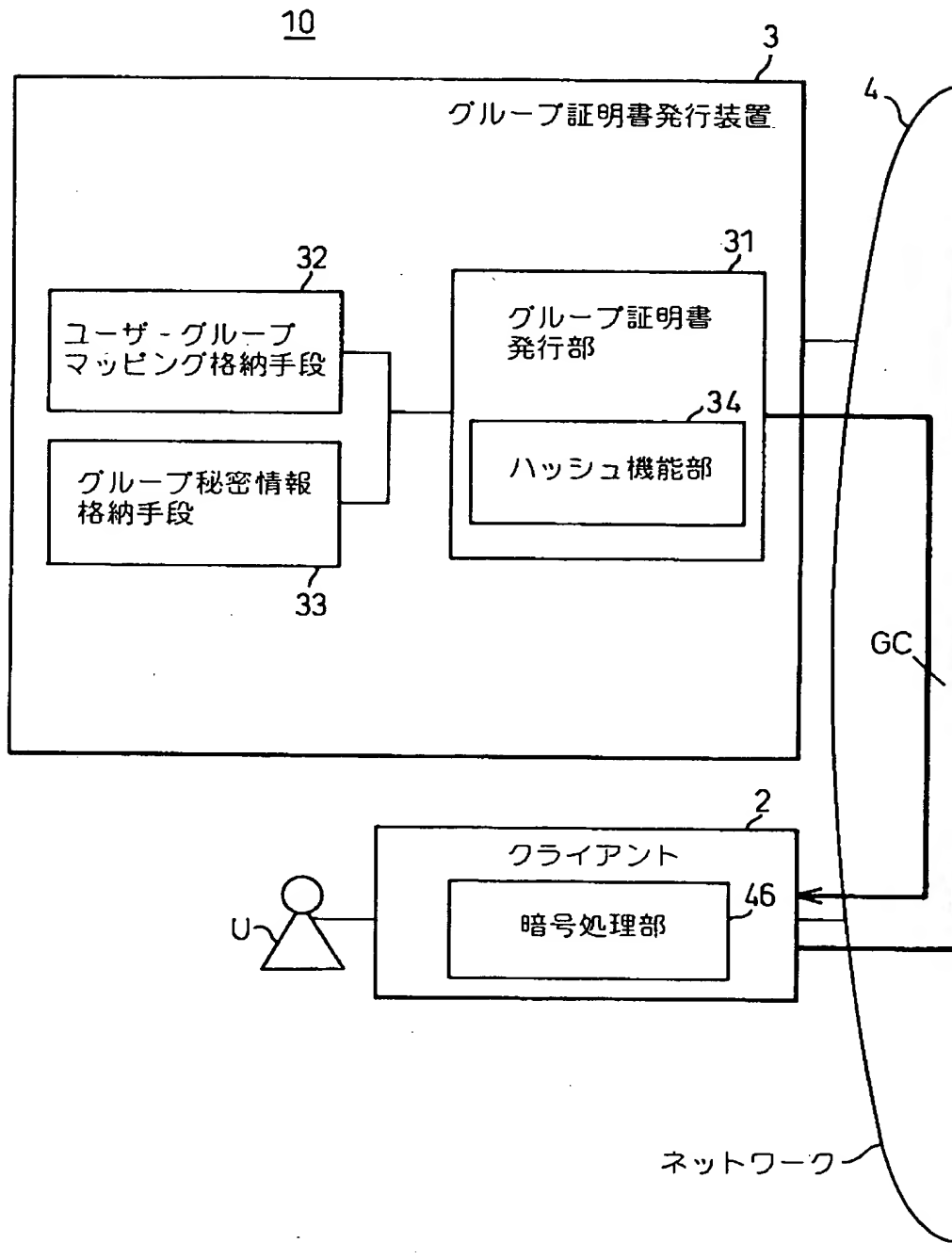


【図 3 1】



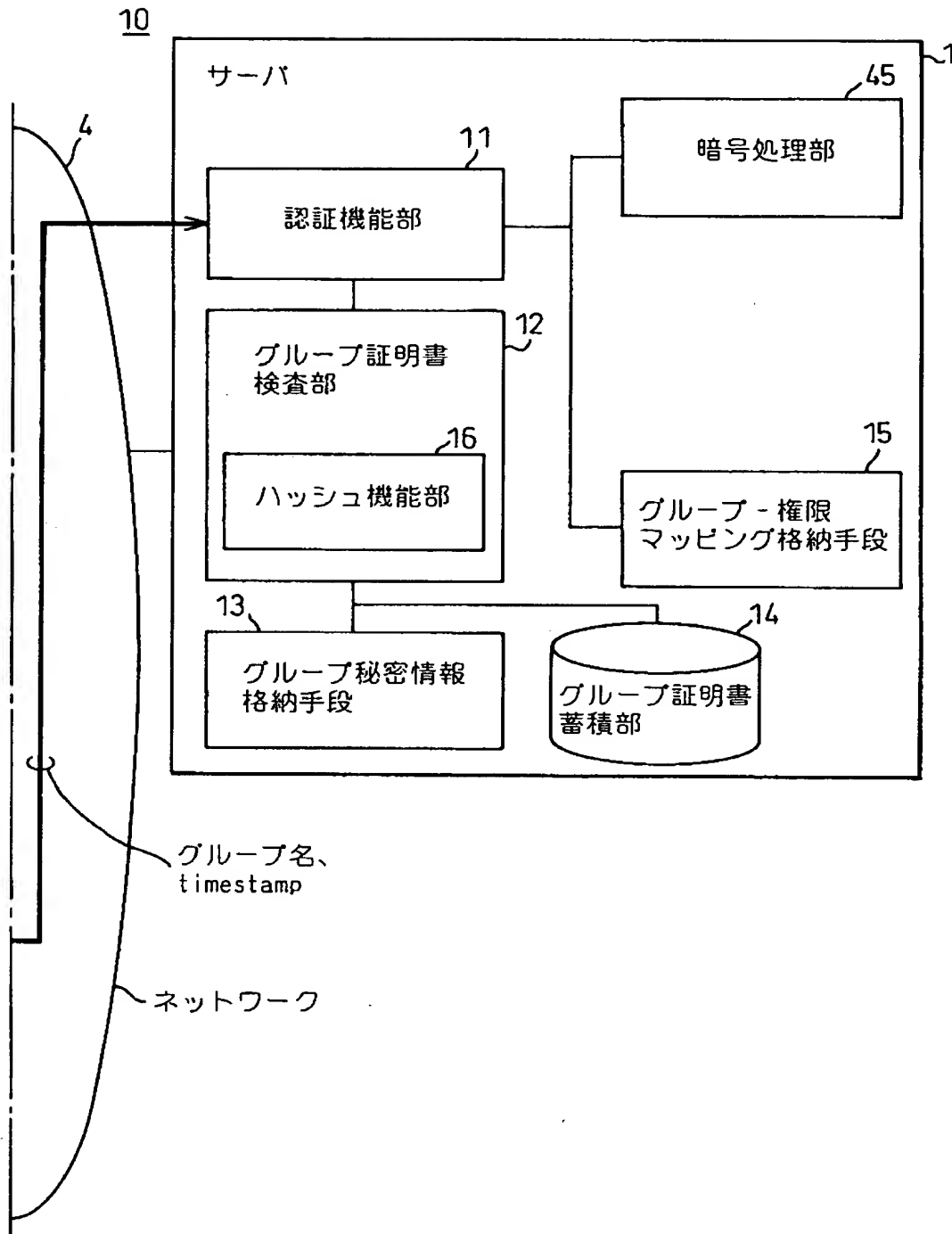
【図 3 2】

図 32 本発明に基づく第 4 実施例を示す図（その 1）



【図 33】

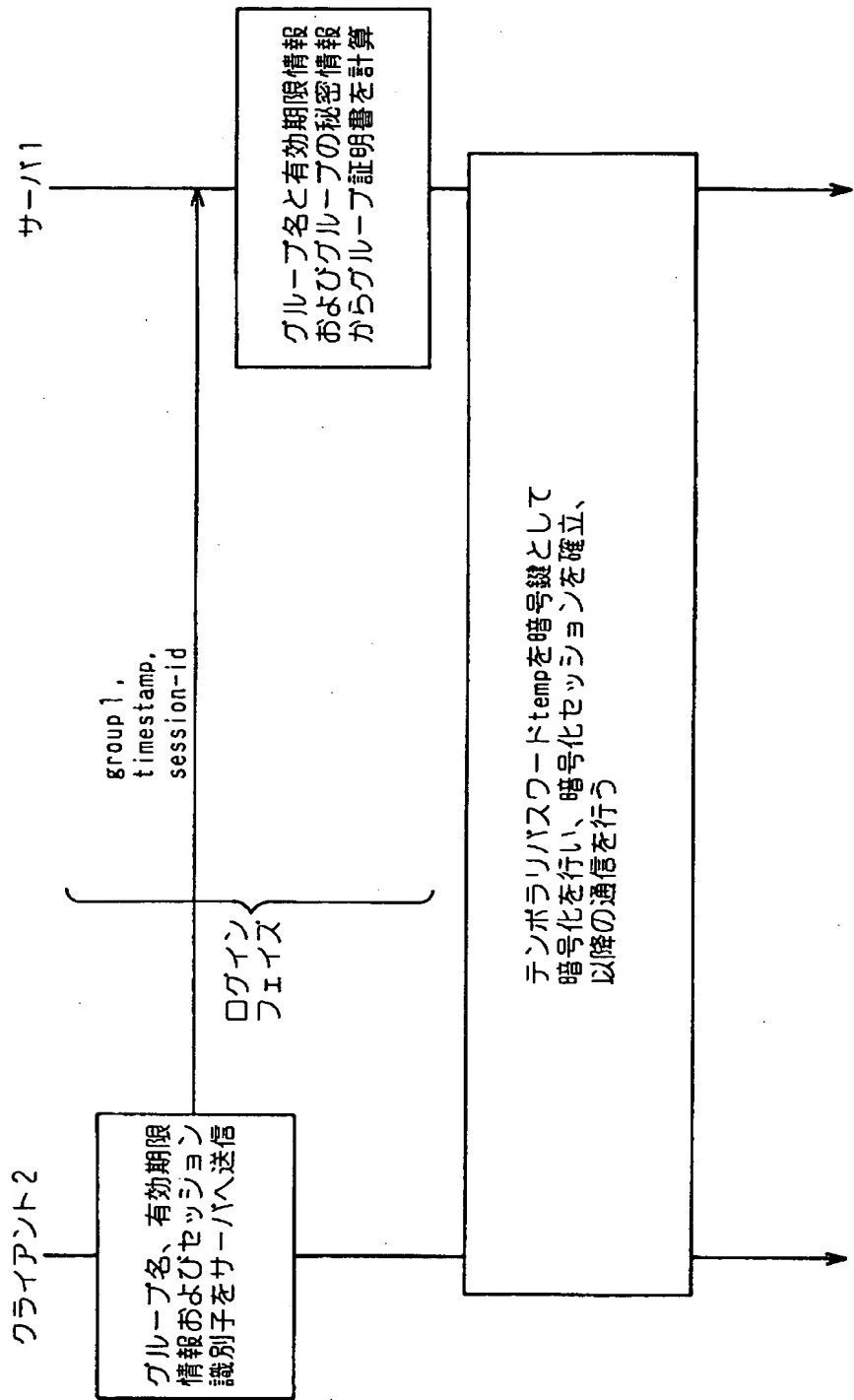
図 33 本発明に基づく第 4 実施例を示す図（その 2）



【図 3 4】

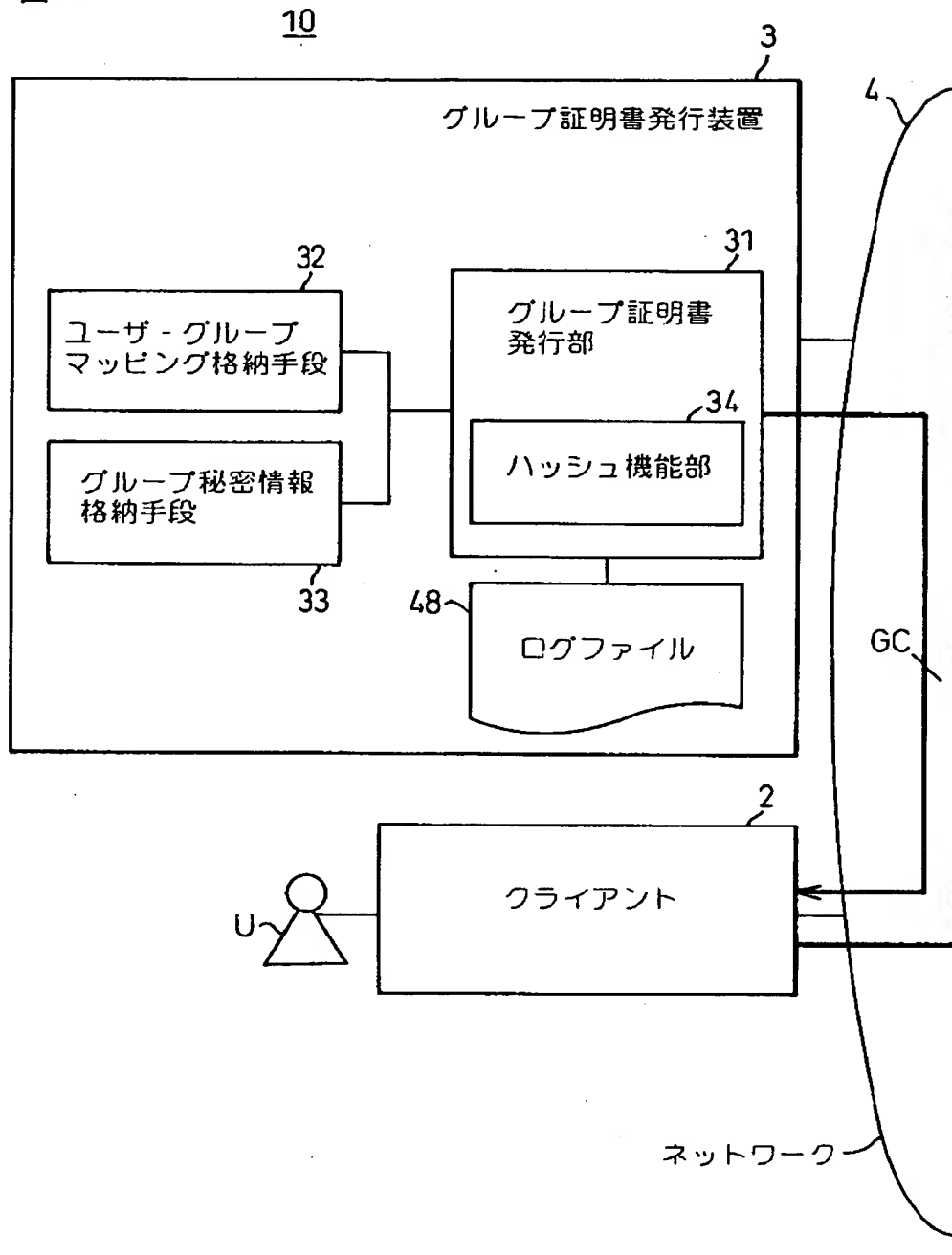
図 34

第 4 実施例のもとでの全体の処理の流れを表す図



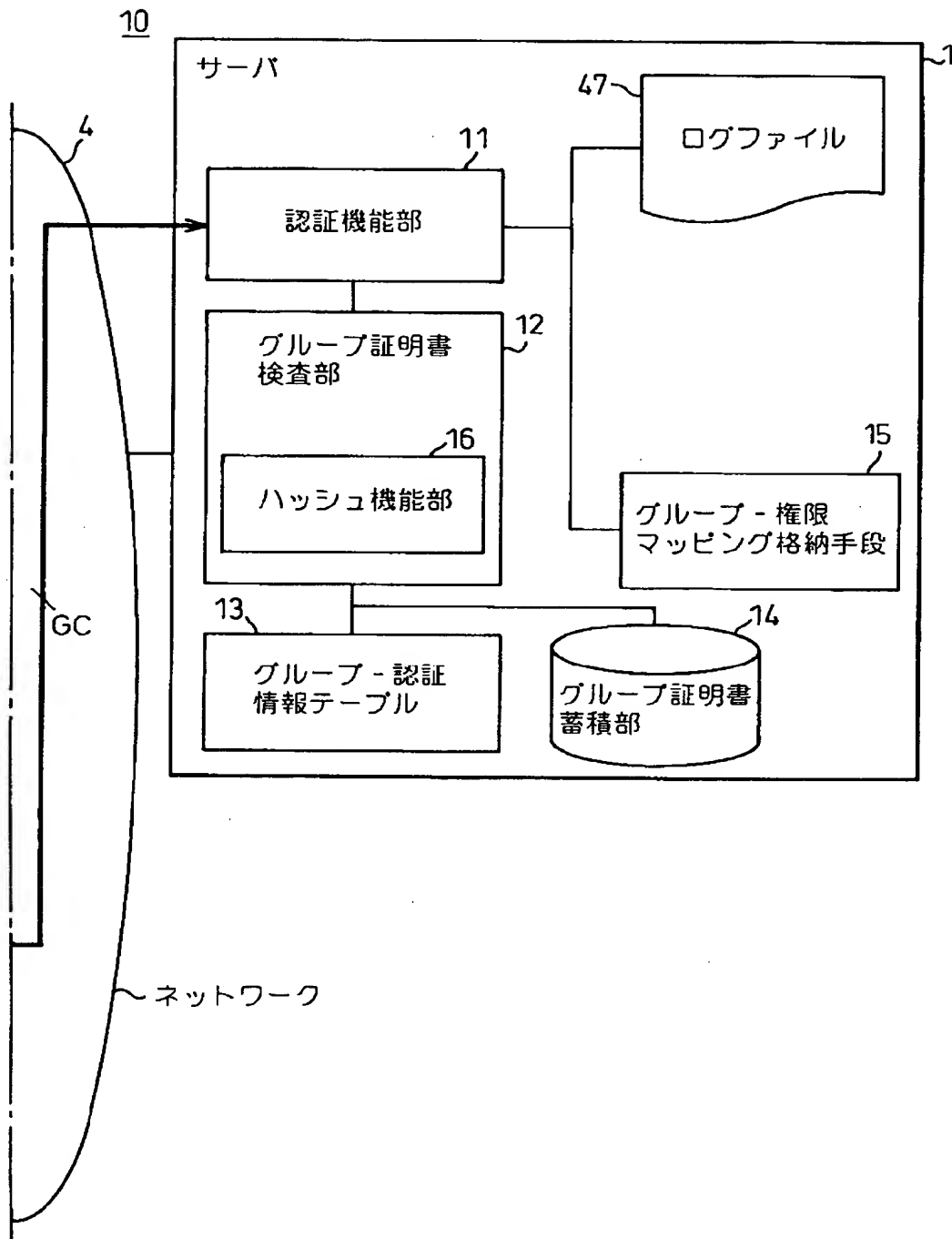
【図 35】

図35 本発明に基づく第5実施例を示す図（その1）



【図 3 6】

図 36 本発明に基づく第 5 実施例を示す図（その 2）



【図 3 7】

図 37

第 5 実施例のグループ証明書発行装置 3 におけるログファイル 48 内のデータの一例を示す図

48

グループ証明書発行装置のログファイル

発行日時	ユーザ	サーバ	グループ	有効期限情報	テンポラリパスワード temp
00/03/01 09:42 00/03/01 10:25 ⋮	user A user B ⋮	server X server X ⋮	group 2 group 1 ⋮	00/03/01 13:00 00/03/01 15:00 ⋮	2983301136 4023502123 ⋮

【図 3 8】

図 38

第 5 実施例のサーバ 1 におけるログファイル 47 内のデータの一例を示す図

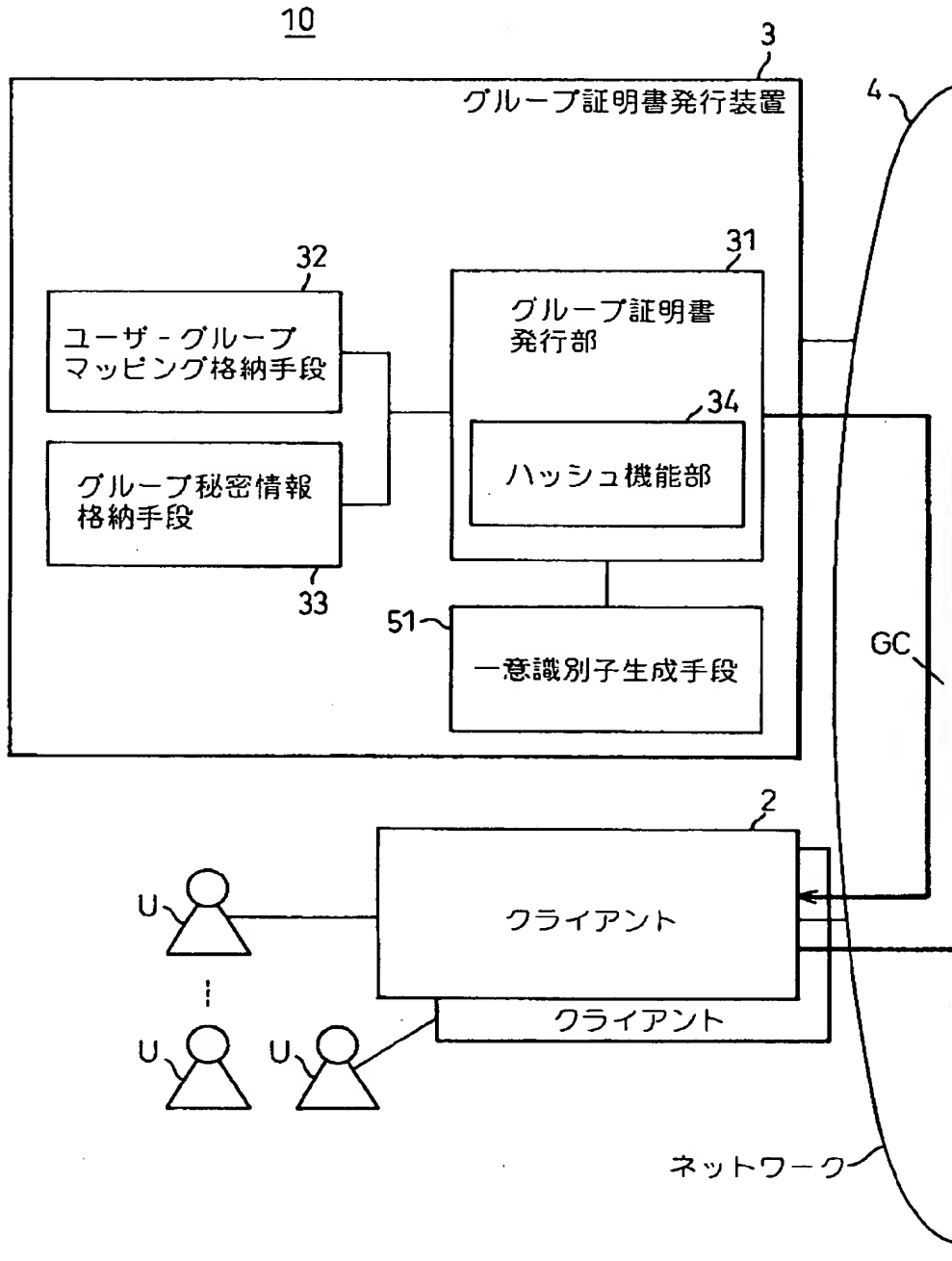
サーバのログファイル

47

処理開始日時	処理終了日時	クライアント ホスト名	グループ	有効期限情報	テンポラリパスワード temp
00/03/01 10:14 00/03/01 10:25 ⋮	00/03/01 12:20 00/03/01 14:41 ⋮	host J host K ⋮	group 2 group 1 ⋮	00/03/01 13:00 00/03/01 15:00 ⋮	2983301136 4023502123 ⋮

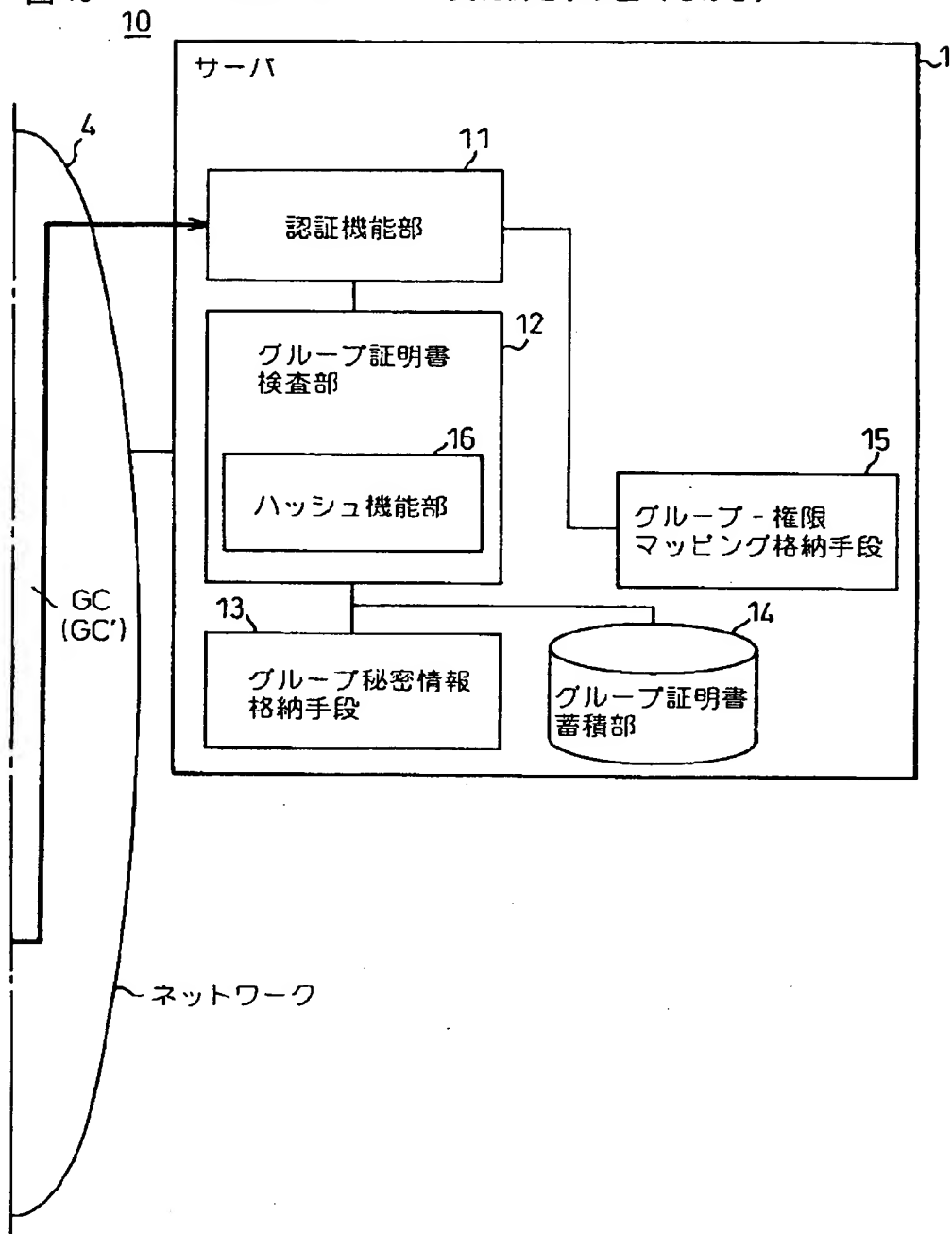
【図 39】

図 39 本発明に基づく第 6 実施例を示す図（その 1）



【図 4 0】

図 40 本発明に基づく第 6 実施例を示す図（その 2）



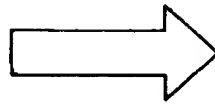
【図 4 1】

図 41

第 6 実施例に基づく証明書識別子 Cid の一例を示す図

有効期限情報 = {有効期限の日時} GC

グループ名 server X.group 1	有効期限情報 00/03/01 15:00	秘密情報 secret 1
---------------------------	--------------------------	------------------

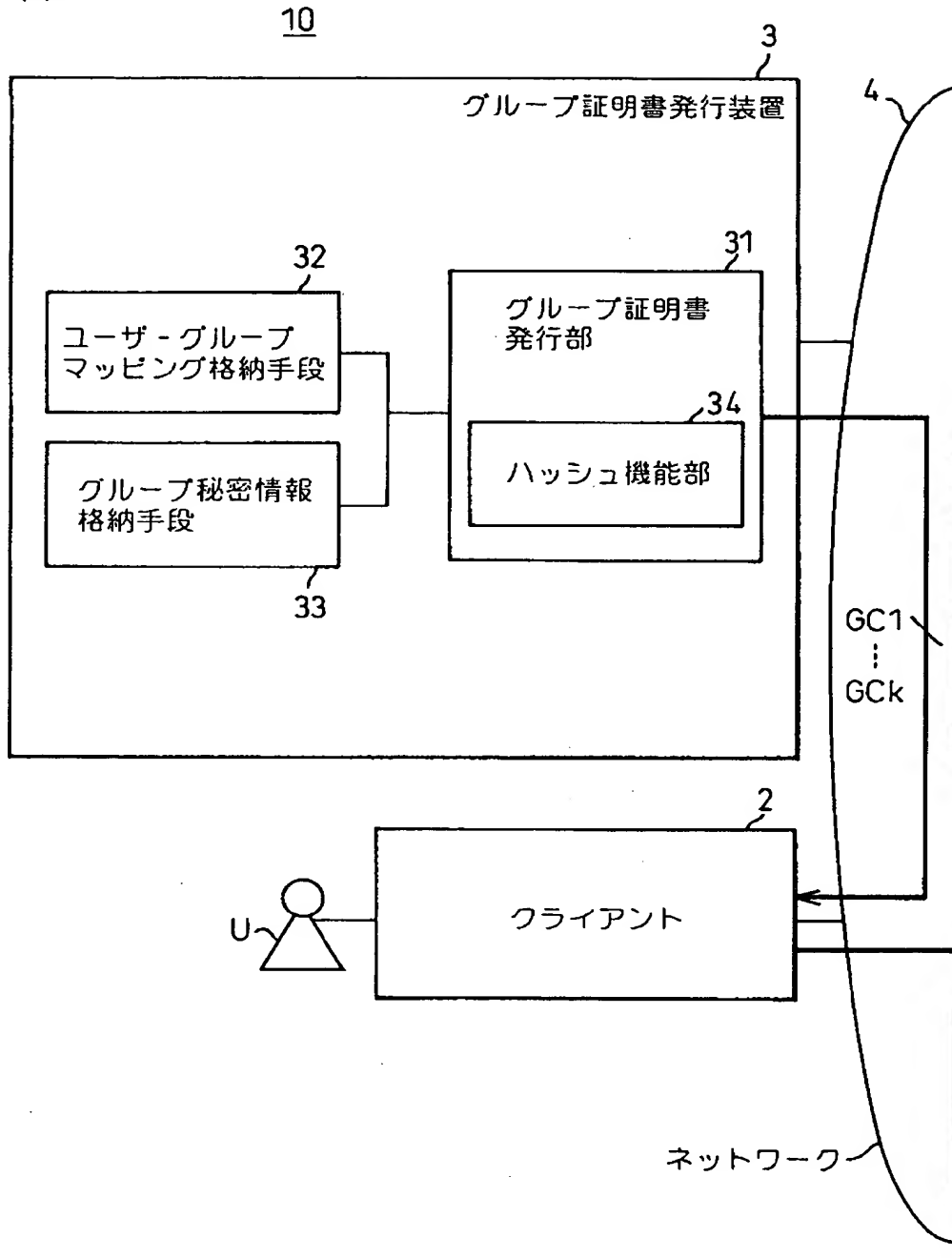


有効期限情報 = {有効期限の日時 + 証明書識別子 Cid}

グループ名 server X.group 1	有効期限情報 00/03/01 15:00	24907435	秘密情報 secret 1	Cid
---------------------------	--------------------------	----------	------------------	-----

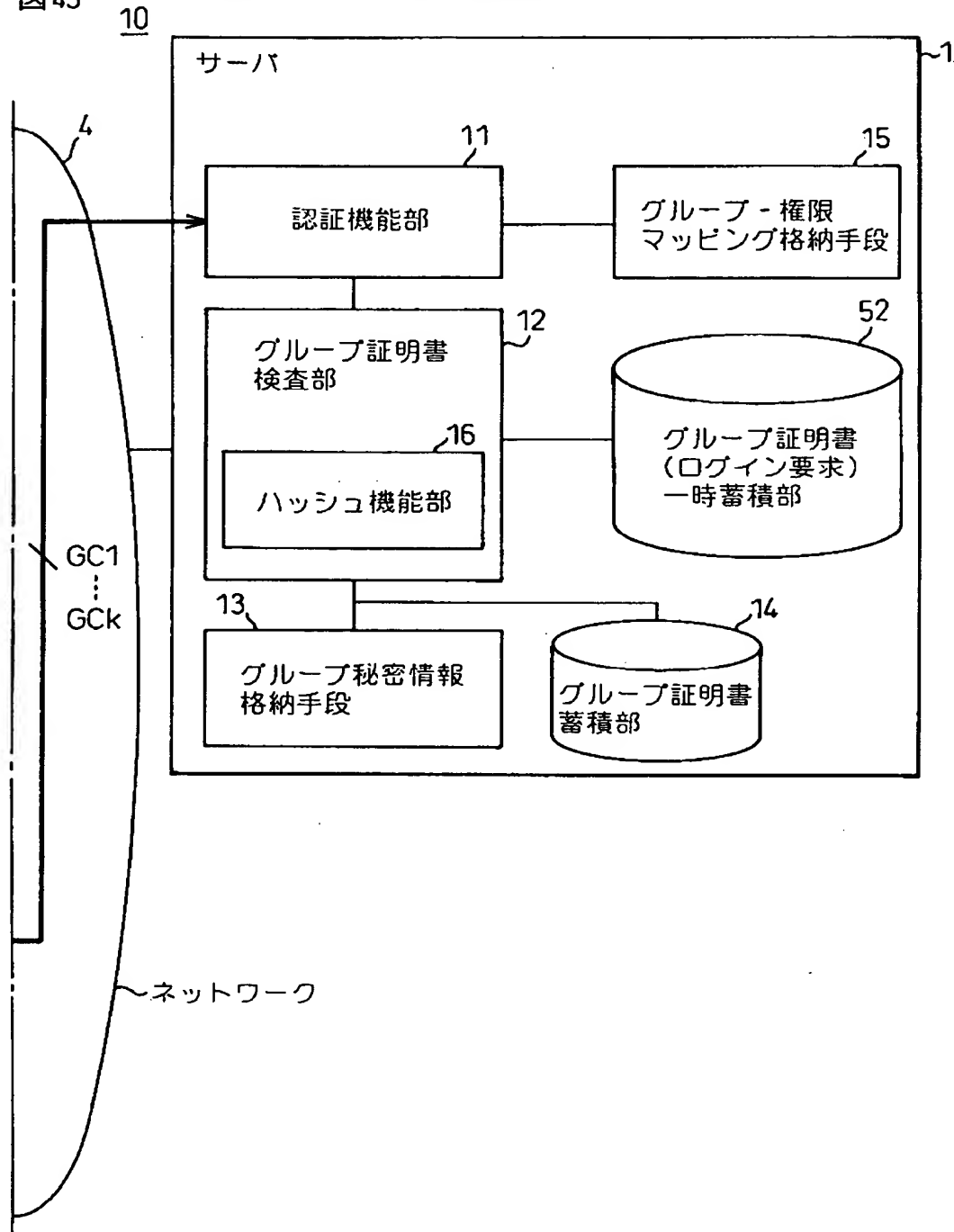
【図 4 2】

図 42 本発明に基づく第 7 実施例を示す図（その 1）



【図 4 3】

図 43 本発明に基づく第 7 実施例を示す図（その 2）




【図 4 4】

図 44

第 7 実施例に基づくユーザ - グループマッピング格納手段 32 内の  
データの一例を示す図

32



ユーザ	グループ
server X . user A	group 3 . group 4
server X . user B	group 1 . group 2 . group 3
server Y . user A	group 4 . group 5
server Y . user C	group 4 . group 3 . group 2
⋮	⋮

【図 4 5】

図 45

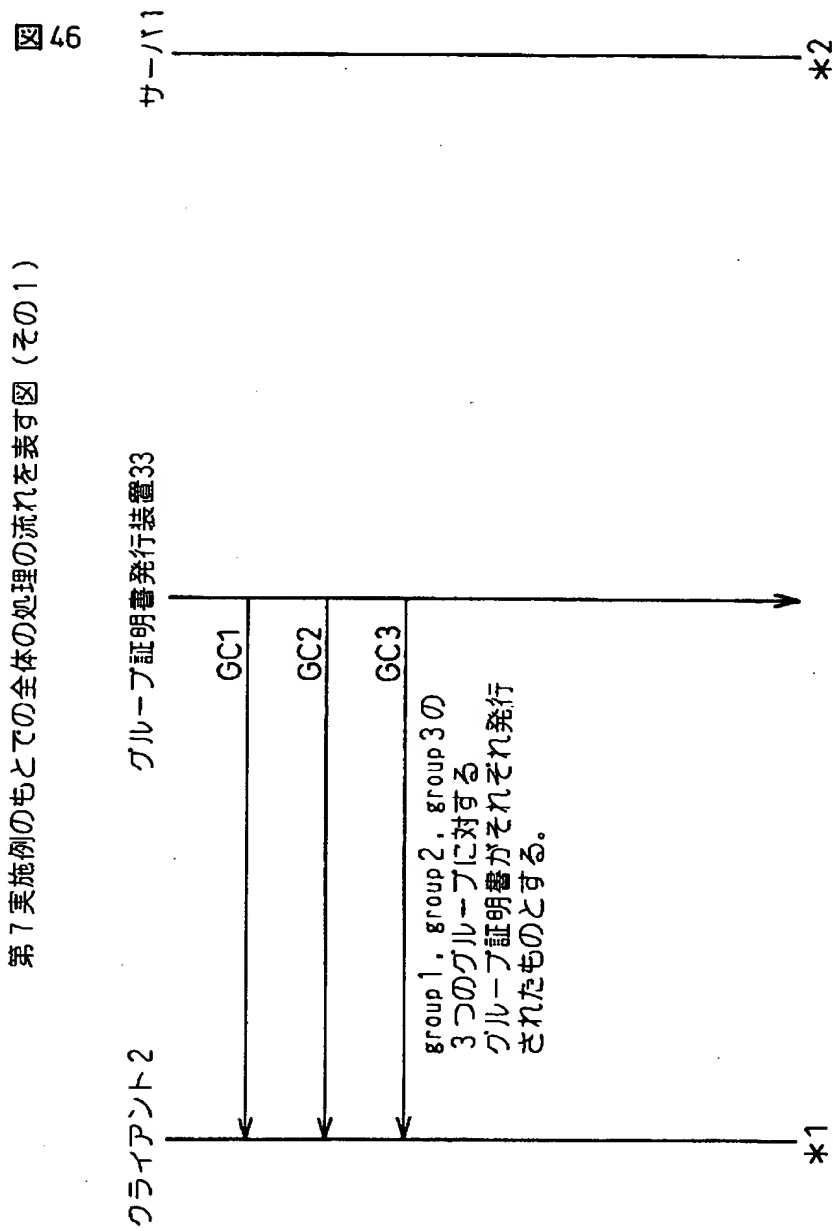
第 7 実施例で採用するグループ証明書一時蓄積部 52 内のデータの一例を示す図

52

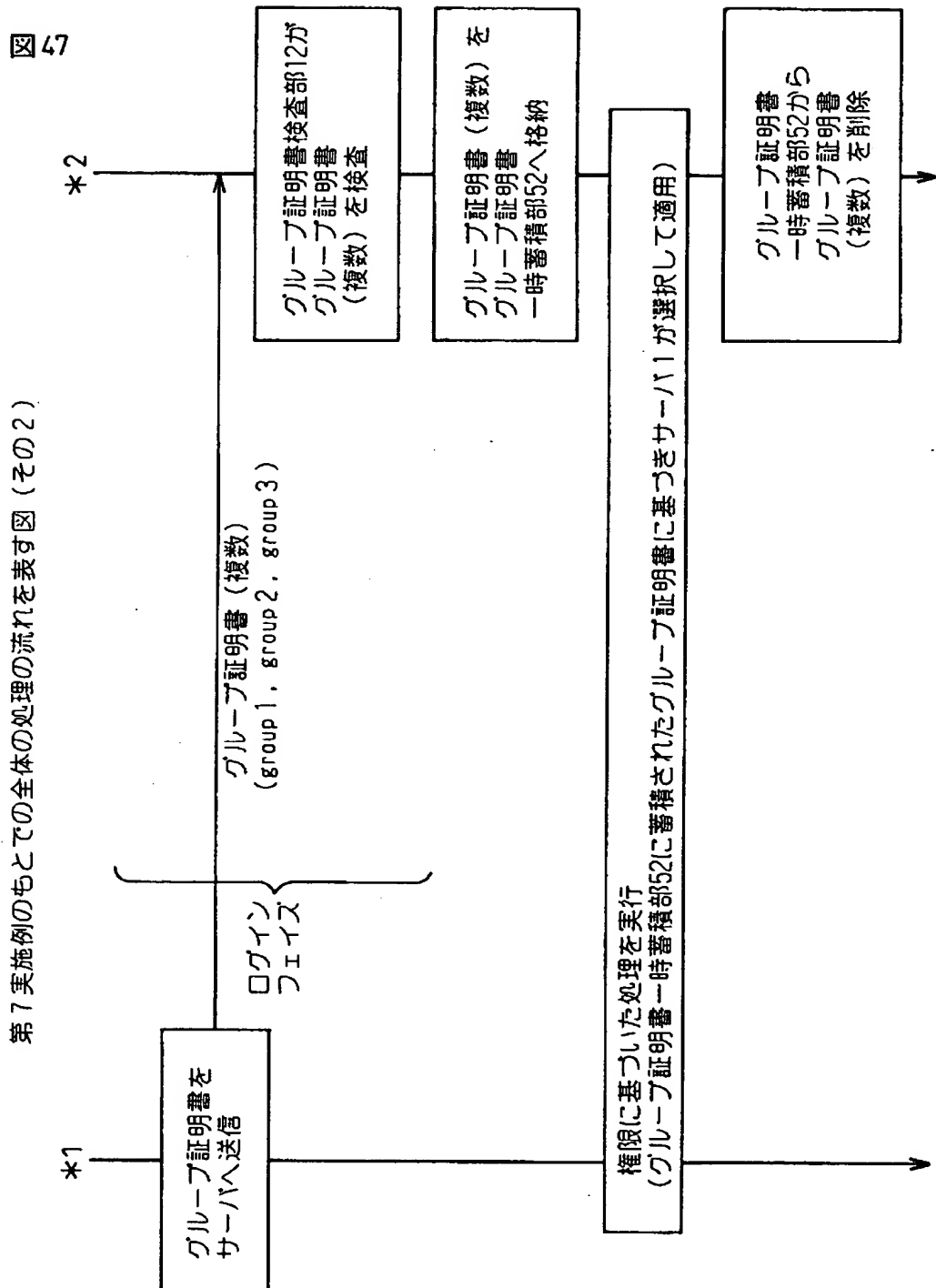
グループ証明書一時蓄積部の保持するデータ

グループ証明書				セッション識別子
グループ名	有効期限情報	time stamp	テンポラリパスワード temp	
server X .group 1	00/03/01 14:00		temp_a	4820100
server X .group 2	00/03/01 14:00		temp_b	4820100
server X .group 3	00/03/01 14:00		temp_c	4820100
server X .group 2	00/03/01 15:00		temp_d	2351121
server X .group 4	00/03/01 15:00		temp_e	2351121
⋮	⋮		⋮	⋮

【図 4 6】

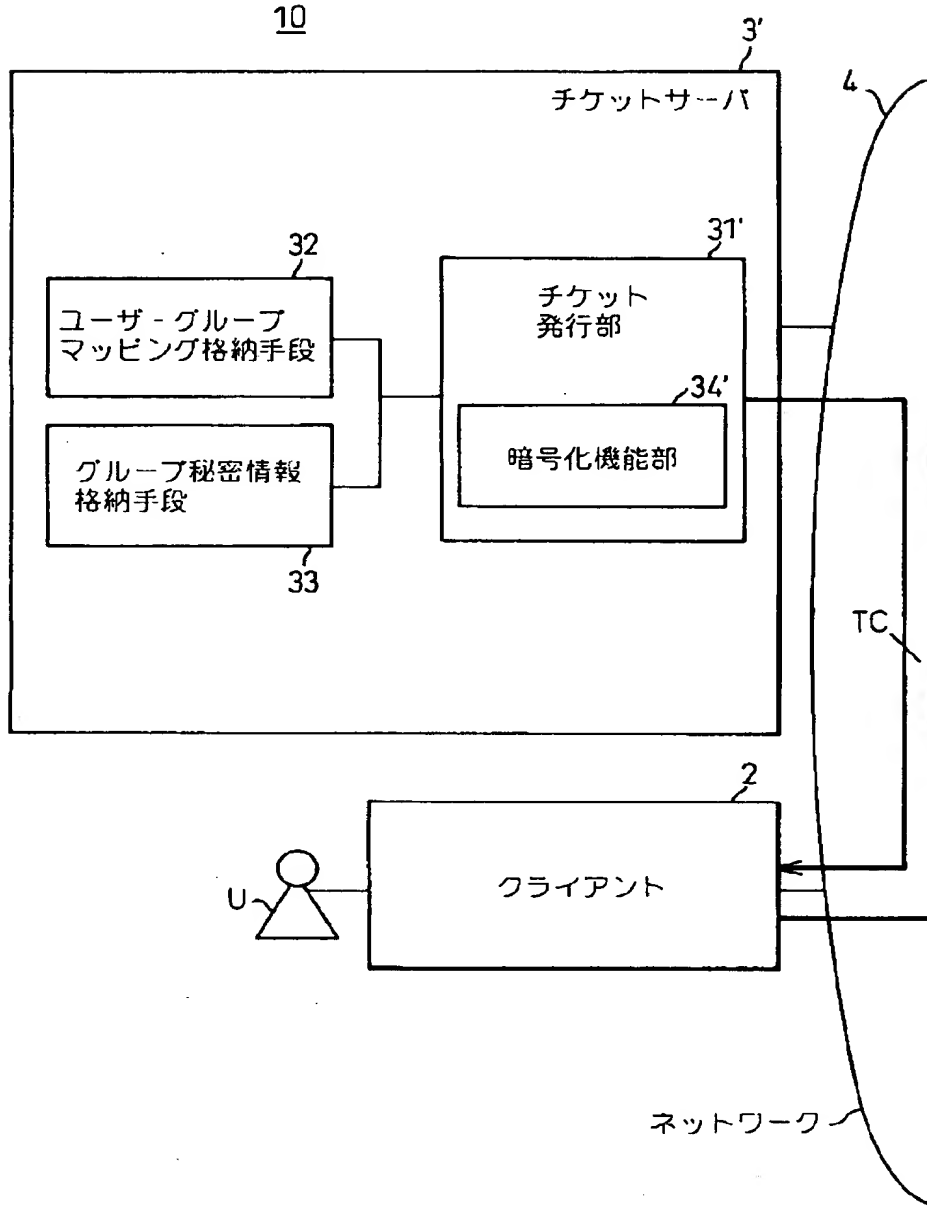


【図 4 7】



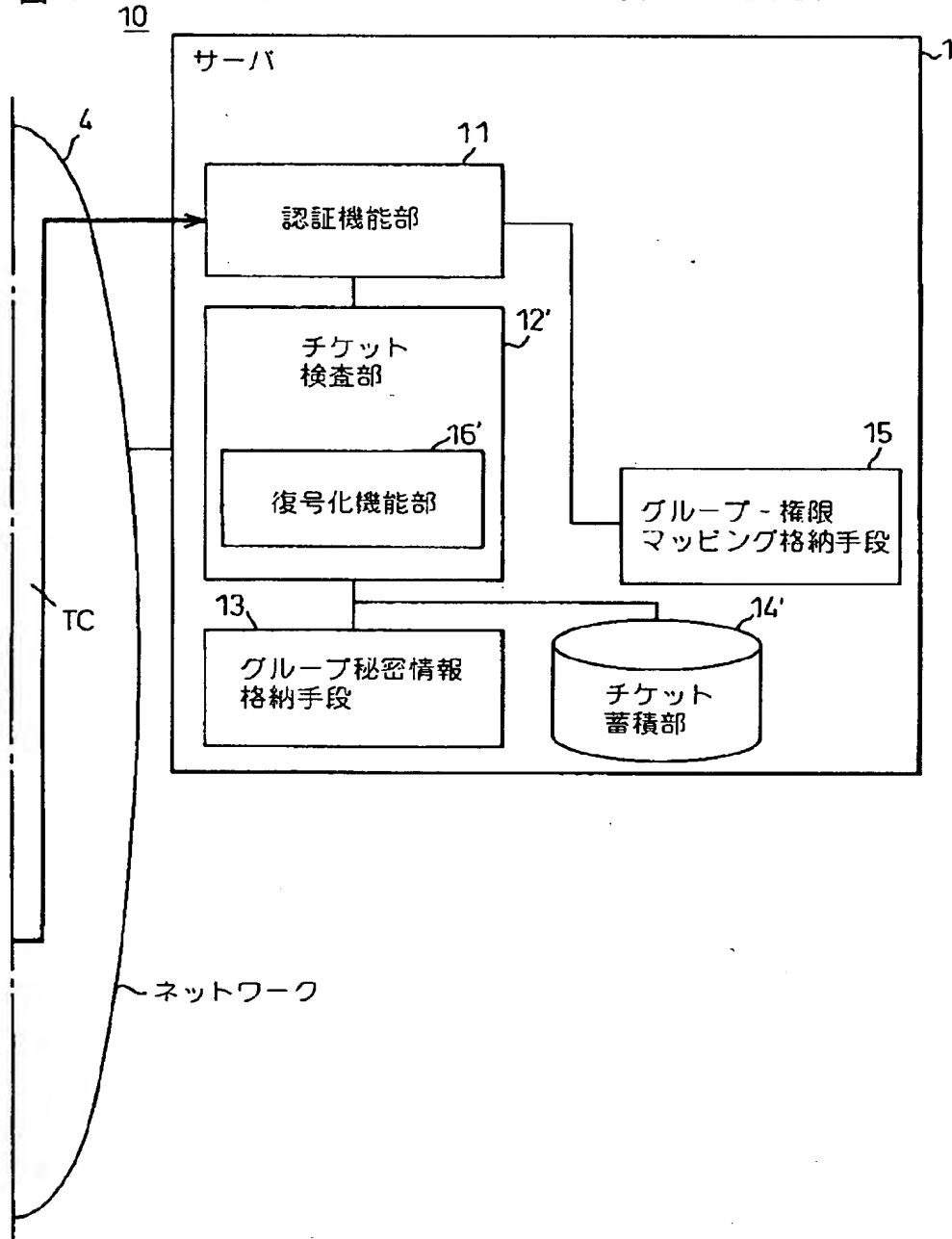
【図 4 8】

図48 従来の分散グループ管理システムを表す図（その1）



【図 4 9】

図 49 従来の分散グループ管理システムを表す図（その 2）



【書類名】 要約書

【要約】

【課題】 分散グループ管理システムにおいて、ユーザの所属するグループに関する認証情報を、クライアント側で高速に生成すると共に、サーバ側でこれを高速に検査可能とする。

【解決手段】 ユーザが所属するグループ名を含む原グループ情報をもとにグループ証明書GCをクライアント2側で発行するグループ証明書発行装置3と、クライアント2側から送信された該証明書GCの正当性をサーバ1内にて検査するグループ証明書検査部12と、を備え、グループ証明書発行装置3は、原グループ情報の情報を暗号学的関数により演算した発行側演算値をこの原グループ情報に付加してグループ証明書GCとし、グループ証明書検査部12は、受信した該証明書GCに含まれる一部の情報を同一の暗号学的関数により演算して検査側演算値を得、発行側演算値と検査側演算値とが一致することを確認して認証を行う。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社